

Center for American Progress



CRITICAL INFRASTRUCTURE SECURITY SERIES:

“NEW STRATEGIES TO PROTECT AMERICA: SAFER PORTS FOR A MORE SECURE ECONOMY”

MODERATOR:

**P.J. CROWLEY, SENIOR FELLOW AND DIRECTOR OF
NATIONAL DEFENSE AND HOMELAND SECURITY,
CENTER FOR AMERICAN PROGRESS**

FEATURING:

**DR. JOSEPH BOUCHARD, EXECUTIVE DIRECTOR,
CENTER FOR HOMELAND SECURITY AND DEFENSE,
ZEL TECHNOLOGIES**

**DR. STEPHEN FLYNN, JEANE J. KIRKPATRICK CHAIR IN
NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN
RELATIONS; AUTHOR, *AMERICA THE VULNERABLE***

**9:00 AM – 10:30 AM
WEDNESDAY, JUNE 15, 2005**

TRANSCRIPT PROVIDED BY
DC TRANSCRIPTION & MEDIA REPURPOSING

MR. P.J. CROWLEY: Ladies and gentlemen, good morning. I'm P.J. Crowley. I'm a senior fellow and director of national defense and homeland security here at the Center for American Progress. And welcome to what is the third in our critical infrastructure security programs, this on port security.

President Bush is fond of saying that to win the war on terror the United States must stay on the offensive. I know of no enterprise where all that matters is a good offense, not even in the NBA. A good offense must be backed by a credible and effective defense. President Bush and Vice President Cheney repeat on a regular basis that we are fighting terrorists in Baghdad so we don't have to confront them in Boston. There is no doubt that foreign terrorists have been drawn to Iraq because of our invasion and occupation, a self-fulfilling central front in the war on terror. However, there is also no doubt that after Iraq a stretched and strained military will require a strategic pause in order to recover, recruit, and reorganize to be more effective in this challenging security environment in which we find ourselves.

Knowing that, the question is whether we are using this intervening period, now almost four years from 9/11, to make our homeland safer. The answer is not wisely enough, and not fast enough. There is no doubt that we have made many military and political targets harder to attack in the aftermath of September 11. We have dramatically increased – here in Washington, for example, we have dramatically increased the setback at the Pentagon for any of us who have served there. We have seen even recently how a small aircraft here in Washington can generate a substantial air defense response. Our ports are different. They must remain accessible. For our economic security, they must remain open. If we are forced to close them in response to a future emergency, what Steve Flynn called a “self-imposed economic embargo,” we will help terrorist organizations like al Qaeda actually achieve their strategic objectives.

Of all the 17 critical infrastructure sectors identified in the interim national infrastructure protection plan, none is more vital to our economy and our way of life than our ports. We are a maritime nation, and no nation on earth benefits more from free trade, global supply chains, and open and secure ports. No one has more to lose if the flow of goods and people across oceans and through borders is interrupted. And yet in the face of terrorism risk that would instantly create billions of dollars in economic loss, the Bush administration chooses to devote only tens of millions of dollars to protect our economy from harm and mitigate the impact of disruption.

Money is an important, but not the only, missing piece in this security puzzle. As we have seen in other critical infrastructure sectors we have studied, we are not sufficiently focused on the management of risk, changing the way that we do business in order to reduce the likelihood of a terrorist attack, and not putting in place redundant and resilient business practices that will minimize the impact, and thus the cost, of a terrorist

attack. And even if the Department of Homeland Security is beginning to shift towards a greater emphasis on risk management – and certainly the testimony that is expected this morning in the area of chemical facilities is a step in the right direction – there is no guarantee that Congress will follow suit. A great deal of effort, as we will hear, is based on theoretical vulnerability and not on risk – what our adversaries are likely to strike and what we can least afford to lose.

One year after implementation of the Maritime Transportation Security Act, or MTSA, it is a good opportunity to take stock of where we are with respect to port security and for that we have invited two of the nation’s preeminent experts on port security and supply chain security to provide their thoughts. Dr. Joe Bouchard, Dr. Steve Flynn, have devoted substantial energy during distinguished military and policy careers to maritime security. Their distinguished biographies are in your packets.

We are honored to welcome them here and I asked Joe to put his thoughts down in a paper that’s in your packet that we are very proud to release today here at the Center for American Progress.

Joe asked me, “Well, how long should it be?” I said, “Well, 15 to 25 pages.” He goes, “That shouldn’t be any problem. My dissertation was 1,200 pages long and Condi Rice was forced to read every single one of them.” (Laughter.)

I’m going to guess that Steve Flynn’s dissertation at the Fletcher School was not quite that long. He has written a shorter, but compelling, account of homeland security and port security called *America the Vulnerable*, which just happens to be for sale outside the door as you leave for those of you who do not already have a copy.

As is our custom here at the Center, we’ll kick around some thoughts here as a panel for a few minutes and then open it up to questions. I do know that there are a couple of media representatives here in attendance and while this is always unfair, we’ll invite the media to kick off the audience questioning when it’s time. When we do open up for questions, please wait for the microphone that Antoine will bring to you and by all means, identify yourself and your organization.

With that as preliminary thoughts, let’s start the discussion. Here we are, one year after MTSA implementation on the domestic side. On the international side, where are we?

Joe, you start off.

DR. JOSEPH BOUCHARD: First of all, my perspective in addressing these issues is not a top-down perspective based on academic research nationwide. I’m heavily involved in one particular port: the port of Hampton Roads. So my starting point is what I see firsthand on the docks down there working with the Coast Guard, working with the longshoremen, and then extrapolating upward to try and look for the trends nationwide affecting all the ports that I have seen on the waterfront down there. So I’ll admit that

this is kind of an inductive – is that the right word? – approach starting with very limited anecdotal observations and then doing research to see how much of that applies nationwide.

I have seen – to try and keep this short, I have three major concerns that I laid out in the paper. First of all, in port security, and maritime security writ large, there is a tremendous strategy/resources mismatch. I know that's a military term, but that reflects my background. The tasks that are required to be accomplished to implement the Maritime Transportation Security Act, MTSA, don't come cheap. And the level of funding that has been made available by the federal government is only a tiny fraction of that amount. The rest is expected to be paid either by the state governments through their port authorities, who are state agencies. If you have any questions about the ability of state governments to absorb it, read any newspaper in Virginia, California, any of the port states, on the financial challenges facing their governments where they are scrambling to come up with enough money for schools, for roads, and at the same time their port authorities are coming to them for increased funding to pay for a federal program.

And then the other is the private sector. The private sector in the port industry – the margins are very low; it's extremely competitive. That's reflected in the very low prices that Wal-Mart and Target and other distributors, other retailers, can offer. Given that competition, given the very low profit margins of the private sector, they are not awash in cash to pay for the MTSA mandate. It's very painful for them. The phrase I like to use just to get people to think about this is “the United States will put an astronaut on Mars long before it achieves effective port security at current funding levels.”

The second problem with the funding side is the way the resources have been allocated. In the past, they have not really been risk-based. It's been very political; spreading the very limited funding as widely as possible. In the current round of port security grants, round five, an initial effort has been made to shift that to a risk-based allocation of funds, but even that is flawed. To its credit, DHS tried to prioritize ports. That is good, but they need to go beyond that and prioritize facilities within ports. Today a very low-risk port facility like a facility that handles cement – if it's in a high-risk port it can get port security grant funding where a liquefied natural gas terminal that's not in a high-risk port cannot. And I'll give you which one is a greater risk, both economically and in terms of mass casualties. That is not reflected in the allocation grants.

And the final problem in resources is the sustainability issue. The port security grant program, the rules of it, only cover about 7 percent – I think that's what I said in my paper – of the cost of implementing MTSA. All the rest is outside the bounds of the grant program. As anyone who has served in the military knows, you always have to think in terms of the life-cycle costs of a program. That has not happened. The current port security strategy embodied in MTSA is not sustainable. Sustaining the level of commitment called for by MTSA is going to be expensive and the resources aren't there.

Anecdotally, and I apologize that I can't provide hard statistics on this, equipment purchased by ports with port security grants is already being taken out of service because

they can't afford to maintain it and operate it. Very high tech, fancy equipment is already either degraded or out of service, and they don't intend to put it back in service because they don't have the money. There is a fix to this, and I'll get to that in just a second.

The second issue is the entire approach needs to be risk-based. Right now, because MTSA focused only on vulnerabilities and everybody is vulnerable, everybody is expected to meet the same very high security standards, whereas only high-risk facilities get money. That exacerbates the resources problem. In reality, not every facility is high risk, and the very simple solution is a low-risk facility should not have to meet the same security standards as a high-risk facility. That cement terminal shouldn't have to meet the same security standards as a liquefied natural gas terminal – very, very simple. That brings their costs, their efforts into line with the risk that they represent. In the paper, I outline that in a lot more detail. I'll spare the details because otherwise P.J. will whack me. (Laughter.)

The third issue I raise – I'm very concerned about – is there is a significant gap between the attention to security and the lack of attention to continuity of operations. The necessity to look at restoring operations is slowly dawning in the minds of officials in DHS, but their initial efforts are not adequate and they don't really have a good understanding of the port industry or the shipping industry and how it works. The emphasis needs to be – needs to go one major step beyond what they're thinking right now, which is they have a security program that is very much oriented towards shutting ports down if there is a problem. The Coast Guard only has three levels of maritime security condition. One, which is normal; two, which imposes extra measures; and three, which shuts everything down. But even level two has very significant impact – very severe impact on ports.

If there is an incident, current policy implicitly assumes that your security response is going to shut everything down, and then you go get a cup of coffee, make sure there's no threat, however many days or weeks that takes, and then you start the recovery process. And the initial planning on how you do that recovery has started. As I said, it's not adequate. What's missing is any conception that you can have a more tailored response that minimizes the degree to which you shut down. To use an old military expression, you degrade gracefully. You just shut down what you absolutely have to, you focus your security response exactly where the threat is, and you allow the commerce to continue so that later on the recovery effort is focused on that specific segment that you did have to interfere with to ensure security. That is the true meaning of continuity of operations.

Now for that to be effective, there needs to be two complementary programs which I outlined in the paper. One is you need to integrate specific actions related to consequence mitigation into your security plans. An example I like to use is in many cases, like an oil terminal, very large investments in security won't buy you anything. On the other hand, very modest investments in engineering enhancements to the terminal or simple things like better berms for containment can drastically reduce the consequences of an attack. So you may not be able to prevent the attack no matter how much money

you spend, but you can prevent terrorists from achieving their objective of massive impact on the economy and mass casualties through much more feasible and affordable measures that reduce the consequences of the attack. Those two approaches need to be integrated into a single, unified approach that allows investment to go where it will do the most to counter the terrorist threat. And then the final part of it is at the business level, especially in the private sector but also with the state agencies, the port authorities. They need to have robust business continuity plans.

One consequence of this risk-based security requirement is some facilities will have to meet less stringent security requirements. In effect, what the federal government would be saying is, “you’re less important to the nation, so we’re going to leave you more vulnerable. And we can live with that because if you’re attacked, it won’t cause mass casualties, it won’t take down the American economy.”

Well, that company, because they get to save money by not having as robust a security program, they darn well better have a robust continuity of business plan and capabilities in case they are affected by a terrorist attack. So that’s a second important element of this overall continuity of operations is everybody – federal, state and local – needs to be on board with continuity of operations.

I think overall the consequence of or the benefits of doing this would be very limited funding will go where it achieves the most benefit for countering a terrorist threat. The burden of the unfunded mandate will be greatly reduced, and our ability to endure, minimize the consequences of, and recover from a terrorist attack will be greatly enhanced.

How’s that for an overview?

MR. CROWLEY: Well done. Well done. Steve, you’re welcome to react to Joe, to elements in his paper, and/or broaden because you’ve been – you’re perhaps the leading voice in terms of global supply chain security, shipping security. How are things looking when you look from – go beyond the United States just to what’s happening around the world?

DR. STEPHEN FLYNN: Well, thank you very much. It’s a pleasure to be here this morning. And I really want to applaud Joe on a superb paper here. I think it’s a very – both gives us a sense of where we are and really provides some very useful, I think, guidance about where we need to go. And so there’s not much disagreement I’m going to have with many of the elements of what’s in here. And let me just point out that I don’t think that’s just a reflection of two former military officers looking at this and converging. It really has been the case – it certainly has been my experience over the last bunches of years, involved with a number of blue ribbon commissions, that everybody who’s outside government on both sides of the aisle, who step back and look at this issue, come to the not very startling conclusion that we’ve got very serious risk associated with our ports and we have very little in place to deal with that risk. But it’s always been a

below-the-radar-screen kind of problem set until quite recently, frankly, and now we're starting to get a handle on it.

Let me just provide maybe three illustrations. On the anecdotal side here, but really sort of highlight some of the stakes in how far we need to go. I'll begin in the heartland of our country, in Memphis – Memphis, Tennessee, where I was just about a little over a month and a half ago. One doesn't think, perhaps, of port security when you talk about Memphis. It turns out that Memphis is, of course, on the Mississippi River. It also is a point where the three major national commercial rail lines, that move all the cargo by rail, meet in Memphis. It's a major railhead and it is the air cargo capital of the world. FedEx runs its operation there. Every 30 seconds there is a FedEx plane going up in the air or landing in its portion of the airport in that neighborhood.

Here's the port security link. Just looking at the FedEx issue here, all of the jet fuel that comes in to feed that airport comes by barge. If you took down a bridge or you disrupted that waterway, within really a matter of a very few days you shut down the air cargo industry, which has some impact on virtually every just-in-time player that moves products around by air. Further upstream, the upper Mississippi, all of the power plants that serve – generate power in Western Pennsylvania, Ohio, and West Virginia are coal and all that comes by barge. We had a bad winter this past year and the waters were basically much higher than they were, caused a lot of disruption. We were about three days away from the power plants going out because they couldn't get the river system back up and running to get the coal there. But happily, they got it within the three-day window that they had.

Move on to L.A., Long Beach, where I was just about three weeks ago. This is a port that brings in 43 percent of all the containers that come in to the country. It also is a place that serves 25 percent of all the energy needs west of the Rocky Mountains. We're in a time of just-in-time refinement. Our refinement capacity is working about 97 to 98 percent. (Unintelligible) we haven't built a new refinery in about 27 years. Basically, as soon as that crude comes in, it's converted and it's into the economy. There are about seven to 10 days of refined fuels in the system in the Southern California area. You close the port down for a couple of weeks to sort things out, literally everybody runs out of gas. That's pretty – that's real challenging to the Southern California economy. It would be anywhere else as well. So even beyond their thinking about supply chain impact, which would also be quite immediate, we have these other linkages across the board.

Now I'll take you over to Hong Kong. World's busiest marine terminal is HIT terminal, Hong Kong International Terminal, run by a company called Hutchison Port Holdings. HIT was built in 1992 to process 3.1 million containers a year, or TEU's – twenty equivalent units. They come in a 40-foot size and a 20-foot size. Today, it's moving 5.5 million on the same footprint. To accomplish this is some of the most extraordinary systems engineering in the world, but it also – as the brilliant Malaysian who gave me the tour of this about almost two years ago quipped, "We no longer take Chinese New Years off." It's a 24/7 operation where at any moment ten panamax or post-panamax container ships; that is, basically big enough to get through the canal or

just too big to get through the canal, are being serviced by three to four gantry cranes per ship with 35 container moves per hour per crane with one-hour slippage between the ships. So when the ship's loaded, it pulls out; the next one's pulled in within an hour. This is going almost continuously 365 days a year. There are lull points, but right now, it's really picking up. It's called the Christmas rush; basically everything that's going to be in our shelves are starting to move in the July to September season.

If the computers go down in that terminal for 30 minutes, the traffic snarls in the port of Hong Kong. If you're down for two hours, you back the trucks up to the Chinese border. This was an extraordinary number I learned there last year, that a typhoon come through and they had to shut the port down for 96 hours. They backed the trucks up 140 miles. And that's between 16,000 and 18,000 trucks backed up nose to nose, with a 96-hour shutdown. This is a very fragile system for disruption.

And while we're thinking in terms of securing it from a gates, guards, and guns perspective, often with just this kill-switch option – either run it or turn it off – we're really, of course, having to deal with a system that is not just local, but is global, where whatever we do here will impact across the board. But where the stakes are just absolutely enormous. Closing our ports for a two-week period will essentially bring the global trade system to its knees, never mind the kinds of disruptions on everyday lives associated with the energy requirements and other kinds of things that are there.

So one would think this would be at the top of the list of issues we would be focused on in terms of national security. And that's why when we see a number like the ones we have in terms of total expenditure for this problem set, it should give one pause. Basically, we're talking on the order of about \$540 million in grants total for all the port security spending since 9/11 from the federal government.

Now why is this so? It is because ports are not run at the federal level; they're run at the state and local level. Most state and localities basically manage them as landlords, leasing them to private sector entities. And the president in his homeland security strategy when it came out in July, 2002, was quite explicit about how resources would be played out in this war on terror. He says that when it comes to critical infrastructure there is, quote, "sufficient market incentive for the private sector to protect itself, and that states and localities need to share the burden of safeguarding that which lies within their jurisdiction. That the core job of the federal government is national defense, what we have over here being deployed over there, and border protection." So we can see immediately why ports would fall on the list. In fact, it wasn't until this year that the president asked for any money for port security because, frankly, the Office of Management and Budget didn't want to get down a slippery slope of being investing in critical infrastructure protection that really was within the scope of state and local and were private owned. That would be a bad precedent from basically the allocation or approach of how they have taken on this.

Now, Joe laid out pretty clearly what the problem is at both the state and local level, and at the private sector level. Those same rules apply abroad. So what we have

essentially is a regime now, and beyond the Maritime Transportation Security Act, in the international environment we have what is called the ISPS code, the International Ship and Port Facility Security code, which went into effect July 1st, which required that everybody had security plans and if you run a terminal or your facilities that the ships had to have complied by certain security rules. And miraculously, every country but five African countries, who can barely find their way out of their own capitals, are compliant with this new mandate because it allows for self-certification. So we essentially have a system where we have a regime on paper, which gives us some level of confidence perhaps that things are happening, where the reality on the ground is there simply aren't incentives in place for people to make any serious investments, nor the same problems that Joe pointed out here, the tendency for this one-size-fits-all approach.

The final area that I would just say is not resource-based that absolutely is at the top of the list, which speaks to Joe's third point, is that there is no plan today at the federal level for how to turn our ports back on should they be shut down. Our captain of the ports, which is a Coast Guard office, have the authority, which they would execute under – particularly if they went to the third-highest level – to close the port down. There is no plan for how to open it back up.

This is analogous to the problem we faced in the Northeast when the lights went out in August 2002, of the electric companies never having thought through how to turn the grid back on. It's not a simple proposition. As we know there, it wasn't just throwing a switch and the power just came surging back on.

The mechanics of shutting it off and turning it back are huge and fundamentally those are management challenges. Those are conversations that have to take place at the local level amongst the public and the private authorities. They have to take place, clearly, at the federal level, and they have to take place at the global level because of the interdependency of these systems. And again, the president has signed a directive as of December 21 this year – last year rather, 2004 – to say “I want a plan” but we're in the “I want a plan” mode nearly four years after 9/11 versus actually having one. So I think that's fairly symptomatic of just how far we need to go with this very urgent issue and, again, hopefully in our conversation we'll flesh out a little more about the prescriptions for how one deals with that.

Thank you.

MR. CROWLEY: Very rich menu. Let me pick up on that last thread. When you look at the grant program, which by the way the federal government wants to eliminate, specific identified grants for ports only and broaden this into the TIP program. But upfront to get from where we were on September 11 and where we are now to a better system of port security, what is the federal responsibility? What should the grant program be aimed at?

And obviously the follow-on question is what's the private sector's responsibility? But primarily, how do you make the grant program the catalyst for

change so that we can get to a better place, encourage market solutions to government imperatives? What should the government be doing? How do you see its role?

DR. BOUCHARD: First, I draw a distinction between the initial implementation and the sustainment, the out-year costs. The port industry started at a very low level of security on 9/11. Primarily because the transition that actually began in the late 60s from break bulk cargo, the classic that you see in that old movies of the nets hauling crates, to containerization are resulted in a drastic decline in theft and pilferage. So the change in the shipping system allowed the port industry and the shipping industry to achieve a huge increase in security and the emphasis on efficiency and cutting costs and transparency, in other words being able to track shipments within the industry, meant that the ports were at a very, very low level of security.

There was still an issue with cargo theft. Some ports were concerned about it more than others, but for the most part it was viewed just like a retailer views shoplifting, as part of the cost of doing business, and as long as it was below a certain level they would live with it. Well, that obviously is not acceptable for homeland security, so passing MTSA and setting standards for security was the right thing to do.

If the federal government wants the ports to be able to achieve those standards in a reasonable amount of time, which keep in mind the deadline for MTSA implementation was 1 July last year and current funding levels, it's, you know, four, 10, 12 decades before enough funding is in place to provide the resources needed to meet that deadline that was a year ago. So for initial implementation it is a wise investment to inject federal funds to very quickly bring everyone up, but that is driven by the time pressure.

Admittedly, some of those funds are going into security upgrades that the port industry should have been doing all along that they didn't do because the cost of that security upgrade was greater than the cost of the relatively low level of theft they had. The Coast Guard estimated in 2002 that it would cost about \$1 billion for the initial implementation for MTSA. The actual cost is going to be closer to \$2 billion. In fairness to the Coast Guard, they tried really hard. They did a very detailed analysis, but it just turns out it's a lot harder to do it right than their initial estimate. If the government is serious about port security then an investment in that initial implementation is a wise thing to do and the Port Security Grant Program needs to be increased to do that.

Sustainment is a different issue. I agree with the concept of partnership. I agree that the private sector and the port authority should be responsible for funding the level of security that's necessary to keep themselves secure; in other words, to implement best practices based on industry standards for protecting their businesses from theft and pilferage, for coping with liability issues – that type of thing. But above and beyond that, MTSA imposes requirements that no business would ever do to protect itself. Those requirements are set to protect the entire nation, not to protect that particular port facility. That incremental cost should be a federal responsibility because it's a federal mandate.

The Virginia Port Authority has been able to quantify that. They had one of the more effective security programs in place prior to 9/11. They had not had a single incident of cargo theft or pilferage in almost 10 years. Their security costs and – so they're representative of the industry standard best practices. Their security costs increased 50 percent when they implemented MTSA. That's not – I'm not talking about the initial investment; I'm talking about the annual operating costs to their security program – increased 50 percent above what it was before. So two thirds to their cost was driven by security they needed in place to protect their business, the other third to their cost was driven purely by MTSA. That's an expense they would not be paying were it not for the MTSA mandate. Every port in the country can quantify that difference.

I would argue that over the long-term that this partnership that is touted by the Department of Homeland Security should include the funding of that partnership. And port should be required to be fund their fair share based on industry best practices and federal government should be required to pay for the share that's necessary to protect the nation as opposed to protecting their business.

DR. FLYNN: To add to that, I think the notion of helping to fund this first-stage compliance with MTSA is essential no just to get from this very low bar where we are to were we need to be in the kind of hurry that the threat would seem to warrant, but also is very much on the international front to just provide some sense of our own credibility as we go out and make the pitch to other countries, many of them poor and less developed, that they need to invest in these same upgrades. And the tradeoffs that we are talking about, of course investing and MTSA compliance, which is mirrored at virtually every other port – you can imagine for a country like a Jamaica with very limited recourses where you have very serious other challenges that this can be a substantial investment that they have to make and the approach that we're taking is a sink-or-swim kind of approach: if you don't meet the standard, we can turn off the switch.

And of course from a counterterrorism standpoint, this is a pretty ineffective threat to carry out because we'll implode their economy and turn (them into?) the very state that we are trying to essentially protect ourselves from. So an investment here in the basic – this baseline level and the federal government helping to jumpstart that process is certainly quite important, but it also is quite critical and is missing entirely from this conversation is to make the case to have the federal government take the lead in helping to migrate this capability around the port.

Our ports, at the end of the day, are on-ramps and off-ramps to the rest of this global economy and dealing with this in a purely domestic context is a bit like hiring a network security manager who says, "I'm only going to protect the server next to my desk." And this – so we need to thinking in terms of how we build this capacity throughout the whole system, and here U.S. leadership in bodies like the World Bank and the regional banks and making an effort to say we need to help build this capacity because we are all – it's as strong as the weakest link is important.

The MTSA was positive in sort of saying we need standards and we need to do it at the federal level because ultimately we can't have a patchwork quilt of requirements and the Coast Guard's efforts to migrate those same requirements into the international arena by working with the UN body called the International Maritime Organization under the ISPF code was certainly appropriate in terms of a tactic to take, but we are just so long from actually having the capability to achieve the standards.

But it's very important to recognize that the transportation industry lives and dies by standards. The box has got to fit on a train, or the ship, or the truck. It's not a negotiable thing, all right. So unlike other kinds of things that we can regulate, which can really accommodate a lot of nuances in the transportation industry – and that's why it tends to be a much slower process. People don't spontaneously make investments in security measures if they think that they are going to end up with daisy chains of other requirements being put on board. So everybody in this industry that I have heard has said we need to set standards and then we also need to have some sense that they're being uniformly enforced for investments to be made.

One of the problems that happened by when we put the ISPF code in place, the Coast Guard was not giving any recourse to actually go out and verify whether anybody is living up to them. Now, on short order what they did is they basically took a bunch of reserve officers whose orders were going to run out at the end of the fiscal year, put them on planes, and essentially do these drive-by checks. Now, some of these folks were not the most skilled maritime inspectors in the world and when they showed up – and basically was to look at the papers that were there, what I've heard from some chief security officers of the major ports is that they actually lost steam as a result of this fly-by validation process because when they went back to their senior management to say we need to continue to make these investments in security, the response was, "Why do we need to do that? We just got the blue-ribbon seal of approval by the Coast Guard coming by. I guess we are good to go." So rather than in fact making this a progressive effort to raise the bar across the board, we put in place a regime that we so quickly declared victory on, that we are actually seeing a stalling out of investment in tackling this very complex problem.

So it's both setting standards and having the capacity to enforce the standards, that is critical, but they final area where I put a lot of emphasis on the grants and it speaks to this whole continuity of operation issue, which we have (not done?), is investments in things like exercises, and lots of them. These is where we really bring stakeholders together and get them to realize what the stakes are and what the problems are. And I – time and again here, you know, this is a town that does not works by facts; it works by anecdote. And you find, sure enough, I just at a hearing I was at most recently, you had the chairman and the ranking member talking about having gone out to top off two and seeing A, B, C and that was why they were doing such and such.

I was at an other meeting recently with Secretary Chertoff where he cited the same experience as motivating from a (unintelligible) pursue yet an other initiative. Exercises can be a very useful investment on a relatively small scale to raise the

visibility, get the buy-in for making things that should strike us as common sense overall. And one which you have to do beyond the local – you have to find ways in which you see these interdependencies across the board.

MR. CROWLEY: Picking upon that point, on continuity of operations what is the government role? You spoke, Joe, in your paper about the prospect that if the worst-case scenario happens, there is some sort of incident, there is this temptation to flip the switch, turn the port off. The instinct would be that the government would in fact try to take over the global shipping responsibility, something for which it is probably not prepared. You know, pick up on that point.

DR. BOUCHARD: The thinking on this right now is – at the federal level appears to be somewhat disjointed and first of all there are no plans. There is no coherent strategy. What I will say is at least there is recognition that continuity of operations needs to be addressed, but beyond that there is not very good understanding.

On the one hand there are these tendencies to think in terms of the federal government trying to control everything; to try and tell the shipping industry where to send their ships, where to send their containers; to develop such comprehensive understanding of port capacity and how it works that the federal government can control it – can orchestrate it. I have seen that come up in some of the early concepts for how the transportation security operations center should be configured to manage the maritime industry.

The federal government needs to stop thinking in those terms. It cannot run the shipping system. It has neither the expertise nor the resources, and if it tries to do it in an emergency it would just make things a heck of a lot worse. To a large degree, the shipping system is self-synchronizing. If there are problems at a particular port or with a particular trade route, whatever the problem, they are going to compensate for that because they have to keep the containers moving. To keep the containers moving, they have to keep the ships moving. So every day on a minute-by-minute basis, the international shipping system is constantly seeking to optimize its performance, and in the event of an emergency it automatically starts doing that. I will give you one guess what the biggest imperilment to doing that would be an emergency involving terrorism: the U.S. federal government.

The U.S. federal government has two key responsibilities to ensure that that self-synchronizing shipping system works effectively. Number one, it has to be willing to share information with the private sector, with the shipping companies and the port industry. Tell it this is what we are going to do. This is how long this port will be impacted or this facility will be impacted. We are worried about a threat to another port, so we don't want you to go there. Make sure that the shipping industry understands the constraints on the system imposed by the federal response to a security threat. Not a good mechanism to do that now, particularly because it requires projecting into the future what's going to be done and both for security concerns and in some cases just no ability to predict what they are going to do because they don't have plans and it's made up ad

hoc, the federal government right now has a very limited capability to help the shipping system be self-synchronizing in order to minimize the impact of a security incident.

Number two, the – even if, say for example, the incident requires at one port would be closed, the shipping system is going to start moving cargo to other ports to try and keep it moving as much as possible. I will give you a second guess: what is going to be the first capacity limiter that impedes the flow of cargo? Is it going to be the number of wharves, the number of cranes, the number of containers per hour they can handle? Nope. The first impediment on capacity of those other ports is going to be federal capabilities, in particular U.S. Customs and Border Protection – their ability to clear cargo – and U.S. Coast Guard – their ability to clear ships. Both are already severely strained now. Let me say, I have nothing but total respect for the Coast Guard men and women and U.S. Customs and Border Protection men and women in our ports doing their jobs. They are working very hard to keep our nation secure. They don't have the resources they need. They do not have enough people. They don't have enough equipment. Both of those agencies are badly underfunded.

In the event of a disruption of the normal shipping system, such as closure of a port, the federal government needs the ability to shift resources to other ports to try and minimize delays caused by this lack of federal resources. If you have to, take your Customs and Coast Guard people out of the port you closed. Maybe not all of them, but shift them to other ports. Or have some type of a national triage system where, say for example, it's tankers, not container ships, that you are worried about: reallocate the resources so you clear those tankers.

There is no conception of this in federal planning right now. Due to the lack of this planning, right now the biggest impediment to resilience in the shipping system, to continuity of operations in the shipping system is the lack of effective federal policies in this area.

DR. FLYNN: Let me highlight the complexity the federal government has in understanding this problem set as well as figuring out how to manage it by a couple of vignettes. One opportunity I had last September to go out to the Port of Singapore – I was invited out there by PSA to address an international board of advisors, which is essentially their customers, they're the CEOs of the twelve largest ocean carrier lines in the world that account for the 90 percent of the ocean carriage in the world. Well, I was struck by the fact that they want to talk about security. It was – the one issue they pointed out there was the biggest sort of market uncertainty for them; both the incident, but also how the federal government – U.S. government was going to manage it, so that was my charge when I got out there was to get them smarter on it.

The other thing that was more startling for me really – it just didn't sink in; I knew it, but it didn't sink in until the doors closed when I looked around the room and realized I was the only American in the room and I could add 8 percent more of the ocean carriage and it would also be foreign owned. There is no other critical infrastructure

where so much of it essentially lies and is managed not only in private hands, but almost exclusively on foreign private hands.

And fast forward: the very first time that senior officials in this government beginning to have this conversation about continuity of operations sat down with the four largest terminal operators in the world who together account for eight out of every ten containers that come into this country. They either originate or pass through – transship through their terminals. The very first time that meeting happened was in February of this year. If I gave a quiz to the invitees, who are people at the top of our government, on this process here of who the four companies are in advance of this meeting here, not one of the would have passed, never mind who the chief executive is who we need to talk to. This would be equivalent like 9/11 happening and having the White House sit room around going, “What are the airlines?” Never mind who runs them.

This is the challenge we have of a very complicated global industry and the immaturity of the federal apparatus to deal with it. Because it was managed at the local/state level; because, as Joe said, it was self-synchronized, there was a very limited federal role. It was a little – the federal roles, even in the Coast Guard’s case, were pieces of the elephant: managing the waterfront portion or the shipping standards, but not the cargo. It was the Coast Guard. Customs handling cargo, which is largely dealing with the shippers – the importers and so forth, but not really dealing with the transportation system.

So the awareness of this very small, but it also speaks to kinds of things that you need to think through the terms of applications and where investments should be made. Hong Kong is involved with the pilot, and they are going out their next week trying to keep this thing alive, where every single container coming in to the busy terminal I described earlier is going through the a gamma ray imaging, is going a radiation portal, and optical character recognition technology is used to take the container number and put it into a database. This is been up and running since January 1st. There’s about 250,000 images sitting in the database that nobody has ever looked at and the U.S. government doesn’t show any inclination to want to look at.

Now, the breakthrough here is the trucks are doing this at 10 miles per hour on average. It’s built into the gate and so it is having no impact on the throughput. Now, why would the port the Hong Kong do this? It’s getting no federal funding to do it. The reason why they are interested in doing it is because essentially they will have a black-box technology. By capturing the data about every container that comes through and have it at least in the database, if something goes wrong you can replay tape and say this was the container and it was this one supply chain that posed the problem, not the whole Port of Hong Kong. And so given their volumes, they expect – the estimate that to deploy this for the entire port that moved 21 million containers last year, the total cost will be \$40 million, which they could recover at about a \$6.50 per-container fee to cover the cost of putting this infrastructure in place.

But there is great resistance to this approach in Washington. One, because there is concern that if the data is collected that somebody will mandate that they actually have to look at them all and not provide the resources to do so and secondly there's an accountability risk: if we don't do it well enough that they can come back to haunt us, and so there is some trepidation about building this capacity. And the thinking here is that, well, we don't need to do that because we are looking at – in the words of our commissioner of customs of border protection – 100 percent if the right 5 percent. We know what the scary 5 percent will be, where the terrorists will go. Well, any assessment, as we know, of the state of our intelligence should conclude that we are not going to be very good at identifying in this industry where the problems are likely to lie.

So building this kind of capability is not just about preventing the one incident and so forth; but it's also about making the system more resilient. And thinking about the port security as not just the about gates, guards, and guns, but ultimately the resiliency of continuity of operations – you start to diminish the value of targeting. These folks don't have unlimited resources; taking out everything simultaneously is something simply they cannot do. They go for the things that are the biggest bang for the buck, and as you start to limit the ability to have that big bang, you can start to chip away at why some segments of this industry make attractive targets versus others. And if that kind of mentality can start to populate our approach here, we will get out of this sort of one-size-fits-all, very expensive gates, guards, and guns approach that we won't finance but it will look – feel good look and then beat up on people for not having done it post the event, to one that actually sustains something that is so critical to our way of life as a way to proceed

MR. CROWLEY: I guess there is both a depressing and potentially enriching aspect to that. At this point, we will shift to questions from the audience. Please make sure you wait for Antoine and the microphone. And we will start, Tyler, no disrespect, but we will start if there are any journalists that have any questions. Otherwise we will come to Tyler Beardsly (ph).

Q: I am Tyler Beardsly. I have a question related technology and Dr. Flynn made me think of it. When he discussed the sort of fragility of the logistics of the situation, one false alarm in a port could potentially back the distribution system up for miles, a lot of the potential solutions that are discussed relate to at the point of departure in the ports, meaning the scanners, sometimes there aren't the funding streams there to be able to pay for the gamma ray scanners and other things in all ports.

How much discussion is under way related to the point of departure actually – the filling of the container itself? Are there any technology solutions under way to create a sensor suite that you drop in every container that has a – you know within cost limitations, that has the – what is supposed to be there? It could test for temperature, humidity, and light, radioactive traces, and then once it comes through a port, if it is scanned – if there are anomalies, rather than stopping the whole port, they could identify and pull out potential cargo. Are there any things that are maybe – that are down the road

that could potentially be solutions at the front end as opposed to waiting until you get to the port?

DR. FLYNN: Sure. Let me say, the overall approach, something that I have been advocating, is you need to take this layered approach of having capabilities across the system. You know, this reality of any security measure, that if it is a single-point approach, it always travels (across the?) diminishing returns. It gets exponentially more expensive for less and less additional security and that what you always get is a displacement problem: the bad guys figure out what you are up to – the capable ones, the ones that we are really worried about, and they just end-run it.

So if you put any sort of single technology fix or other kinds of things in place, ultimately it's like the radar detector battles of the highways. You know, all the time you get into this race here. So in thinking about this problem set – and it also – the reverse of layers is taking the advantage of something we know from the law of probabilities: if I have five 60-percent solutions but they are all tethered together as a system, I get a 99-percent effectiveness rate. So I don't need perfect security at every level here; I just need pretty good capability, but I have to have it integrated across the system.

So clearly the first thing – place to start is the point of stuffing and this is the – everybody acknowledges the weakest part of our security system. Nobody knows what is in the box. In my recent trip to Hong Kong where I am looking at this pilot program, on the way there I am literally walking from the subway station – I have to go under this underpass where most the traffic is moving to the terminal, where most of the employees are going through a chain link fence and I am looking at this underpass and there is these open container with the fork lift, with a couple of trucks with freight all over the place. This is a consolidator who is stuffing a container in a state of nature right outside the terminal. I quipped with a colleague, I was there – I bet he's a CT PAT (ph) plank owner. (Laughter.) But the reality is the actual stuffing of the container is done in that kind of environment everywhere in the world we have no idea what the security – and once it's closed, it's pretty much off to the races.

So we need a system by basically we say, folks – and CT (unintelligible) to do this, to say you need to go back and do this, but we need to validate it. And a basic approach here is simply third-party auditing functions: bonded players who go out and look at your processes and make sure you are doing basic 101 security measures.

The second piece is tracking the container: its position and its integrity. And here an initiative called Operation Safe Commerce was designed to essentially steel test some of these things and it turned out a big pusher for this – and there was great resistance on this one as well for a year after – from federal government for long time, but the notion here was, one, to winnow out the witchdoctors that are out there. There are all sorts of folks who say, "I have the way to solve world hunger with this technology tool and this is a great device. We use it in trains. It could work everywhere." Well, it turns out it doesn't work with salt water. You know, it doesn't work when you get the G's you drop

from 140 feet down along here. You shake that thing up a little bit here and it just doesn't work.

So we needed to find that out and Operation Safe Commerce was about taking these technologies and applying it and it was a grant program that was ushered through by Senator Patty Murray of Washington, but we did this crazy thing of putting all the results into the cone of silence. All right, TSA was managing it, but we can't tell anybody what we actually found out, so we can have no independent audit. I haven't seen it. Even though involved with some of the orchestration of getting it started, I can't see it because I am not cleared to see it anymore. So we can't learn these lessons and probably the industry can't learn these lessons because of the security kind of measure.

But there clearly are applications for tracking and for sensors built into the container. The possibility is only about two companies in the world that actually make boxes, containers – 40-foot containers. The cost of them is just under \$5,000; actually down around \$3,500 apiece brand new. And building this in the factory is something you could migrate into the system over time but you would certainly want to make sure it works and false alarm problems aren't there.

The third piece is the kind of things we are doing in Hong Kong. There's sort of a disconnection. It's almost feel-good and just kind of wackiness: we are making a huge investment in radiation portals. This is basically a Department of Energy program called the second line of defense or the Megaport Initiative. Radiation portals are an interesting technology; their only limitation is they don't help us with the loose nuke. They won't help us with a shielded radiation dispersal device – a dirty bomb, and they won't help us with highly enriched uranium. But other than that, this is a great program. We are spending \$800 million on it. The reason why is basically the natural occurring background radiation is higher than what you would have – a nuclear weapon is designed to be handled, so it doesn't give off any radiation. Shielding RDD is not a very heavy lift; basically plenty of lead. And highly enriched uranium has such a long half-life that it basically doesn't give off enough that's typically above a threshold to be readily detected.

But when you put a radiation portal in place, at least for the loose nuke and the RDD, it forces the shielding and then you can see the image. So the technology application starts to make sense to have a radiation portal and then have an image afterwards here because then I can see there is a big lumpy object where there is supposed to be Nike sneakers. Okay? (Laughter.) If I didn't have the radiation portal, I wouldn't have to shield and it would be much smaller, so in combination – but the scanning program is handled by Customs and Border Protection; doesn't have much money, so they use it for the right 5 percent. DOE is doing this massive dispersal of radiation portals that are disconnected with this. And, you know, not surprisingly it starts to blow circuits in terms of what are we spending and why are we spending it and do we have a plan? But it really is because these agencies aren't looking at this systematically and causing the problem. That is the third phase.

The fourth is actual (track the?) ship and its condition. The fifth is you spot check at transshipment arrival. Not if it's a 100-percent system across the board, but these folks don't have unlimited resources to get us. It is not like they got the Soviet arsenal in their pockets, all right. It may take two to three years to acquire a weapon of mass destruction or to build one in as an RDD. You got to put in a system where there is even better than half odds that you're going to be detected. And a case may be no, and that it would be displaced. Well, that could be – say we have a maritime threat; it could be it comes in fishing boat then or a yacht. That doesn't solve the problem of a weapon of mass destruction getting in the United States potentially being set off, but it does solve the problem of the consequence of that not being to shut down the global trade system.

You start to manage the risk in ways which – and we tend (not?) to have – this is a resource issue. You want to track essentially noncommercial vessels, you can do that. You just need more Coast Guard patrols and other kind of things and you can do that without causing real disruption.

So these are the kinds of approaches that we need to take and there is a lot there, but there has been a great reluctance to do this. And overall we're operating from – as P.J. was saying at the outset, we have now solidified with the election, “We do it over there so we don't have to do it here. We need to take to battle the enemy. We need to eliminate them in Baghdad so we don't have to fight them here,” and this is all premised that we actually have the intelligence about where they are and what they are operating on, but we have all the eggs in the offense basket. And given the reality that it will probably be 10 years or more if we're working it harder than we are to get our intelligence house in order, that we will get the tactical intelligence, we should have a fallback position when it comes to the things that are most critical to our way of our life like our port and maritime system.

MR. CROWLEY: Back in the back.

Q: Anne Witkowsky, CSIS. A question for both Joe and Steve. Very interested in your comments on recovery and the need for enhancing resilience in the system, so I want to know if you have taken your thinking to the next step yet. That is to say, you put your – imagine yourselves back in the White House, say HSC, NSC. Event's taken place; ports shut down. What are the fundamental pieces of information or processes and processes that you think would need to be in place to allow you to implement an effective recovery process?

So what I mean by that is, for example, the completion of vulnerability assessments and the necessary enhancements to the ports so you have a national picture on the analytical side. On the process side, not necessarily the interagency process, which we understand pretty well, but how you would see partnering with the industry in a case where, as you have pointed out, the federal government has a limited role. Maybe the answer to that question depends on whether we are talking about the ports and/or the shippers, so a process for and plan for enhancing the way we do recovery.

MR. BOUCHARD: Well, first let me say, Anne, that if you understand the interagency process, you are a much better person than I am, which goes without saying. And also as an aside, I still haven't forgiven you for having a baby during the middle of the landmine issue. (Laughter.)

Q: I owe you. (Laughter.)

MR. BOUCHARD: First of all, keep in mind that my practical experience these days is down on the piers, and from that perspective you look up to the White House with fear and trepidation because they have a lot of power to make decisions that are really going to make life hard for you, but not necessarily a lot of incentive to make decisions that are going to help you recover. If in a future terrorist incident the political dynamics work in the same direction as they did on 9/11, the incentive is going to be to take very grand gestures that shows that were taking dramatic action to protect our country, like shutting down all the ports – very massive efforts that are very visible, easily understandable to NASCAR fans, but measures which may not do anything to prevent further terrorist attacks, which in fact in many cases would make it harder to prevent further terrorist attacks. It might delay them, but it provides a strong incentive for the terrorist to shift to a different mode of attack, as Stephen was suggesting.

What is needed is what is hardest to do at that level, and that is very precise measures. That requires, first of all, very good intelligence and very good integration of that intelligence from all sources. And not just intelligence, but information from the private sector and having very robust analytical tools and decision aids to use that intelligence. In other words, to take the situation we have on any given day, which is an abundance of very ambiguous indicators and potential indicators and rumors, and systematically understand them in the context of whether or not they indicate execution of a particular mode of attack.

If you've had an incident, you need to have the ability to go back to that morass ambiguous information, based on what you know about the one incident, and then start prioritizing. Are there other attacks in progress? Was this one of four, or was it just a single attack? What indications do I have, based on what I know concretely about this incident, tell me there is a threat to other ports or to other tankers or other cruise ships – whatever it is?

That is very difficult to do and I will flat say we can't do it today. So no matter how good the intentions are at that level, they end up by default having to forego measures which might be highly effective because they are focused on a specific target set, whether it's ports or ships or segments of the economy – forced to forego that to go to the more draconian measures, which can be implemented in the absence of good intelligence, in the absence of robust analytical tools and skills.

The second thing they need is they need to understand the consequences of government decisions. On 9/11, the loss to the U.S. economy from government decisions was much greater – an order magnitude greater – than the loss caused by the terrorists.

The federal government amplified the impact of the 9/11 attacks. A draconian response to a port of maritime security emergency such as shutting down all the ports or shutting down all the Gulf Coast ports or stopping all the tanker flow because there was an attack on a tanker would amplify the impact of what in fact could be a very small incident; you know, one we could just brush off. “Ha ha. You know. They chose the wrong target. We can live without that ship.” We wouldn’t do that in reality; I know that’s politically inappropriate. But if we take draconian measures in response to that, we greatly amplify the impact and I hate to say it, but if I were a terrorist from what I have read in the press I would have a very strong incentive to attack a port or to attack the maritime industry and I would assume that the federal government will amplify my – the impact of my attack well beyond anything I could possibly achieve with my very limited resources.

So those are the types of things at that level that need to be considered. It is very difficult it requires a change of mindset and it requires much more robust information integration capabilities than we have now or we are likely to have in the near future.

MR. CROWLEY: Let me pick up on that point for a second, Steve. If one of the mechanisms for getting greater system visibility so you can identify that component that is – it may have failed in a particular emergency, but then let the rest of the system go – certainly what you just described as the pilot program in HIT is part of that solution, but is that something that can in essence bubble from the bottom up? From the private sector and then get broader acceptance that forces the government to recognize it? Or is that something that has to be top-down driven? How do you get from a pilot program in Hong Kong to something broader that can have meaningful impact in the scenario that Joe just described?

DR. FLYNN: Well, there clearly has to be a convergence. One of the problems right now is the Hong Kong pilot will stop on August because they have no customer for what they’re doing, which is the U.S. government hasn’t said that it’s good bad or indifferent. There are invested about \$5 million amongst the parties to create a process that would serve the targeting function for the U.S. government and also a restart function but without anybody in the U.S. government telling them that that is in fact what they’ll do with the data, it doesn’t make much sense to improve it so there is market incentives often to create the capability but if there isn’t in fact a convergence of the public sector saying “we understand the capability you are providing, we may need these tweaks” and ultimately want to populate that.

If it comes in place there, and we’re blessed, the next step would likely be that Singapore will adopt the same system. They’re actually using the same model on their Malaysian border. They’ll likely (walk?) it in to their own port, once Honk Kong does, they’re very competitive market. HIT is owned by Hutchison (Port Holdings?), it owns 39 ports around the world, basically moves about 49 million containers. So just as a company decision they could populate, that’s 90% of Rotterdam, both sides of the canal, (Felix Style??) the main container terminal here. So a company decision could just be: “we’ll do it”. If there’s a cost recovery we’ll put the system in place because we see the value of tracking data to support the (inaudible) disrupting the supply chain and if

something goes wrong to allow a nuanced response versus a meltdown response they would have the incentive but they need someone in the U.S. government to say: “this is desirable behavior” and we have not yet got that. But on the issue of the overall “how do you put this in place”, there’s a quip for those of us that are in the port business here: “if you’ve seen a port, you’ve seen a port”, they’re all different and so one of the problems here at the federal, sort of, approach is sort of like airplane kind of response.

Let’s remember, as Joe has sort of highlighted, remember what happened on 9/11, we brought the entire air fleet down and we went through every single airplane to verify there was no terrorists (or means of terrorists?) on it, which took three days – it really was extraordinary that we could scramble to do that – and then we said “all clear” and we began to restart it. But then we did very silly things like put National Guard guys with automatic weapons in the terminals. I don’t know, as a former military officer, there’s nothing more frightening for me than seeing a young testosterone driven young person with an automatic weapon in an environment that they are clueless except maybe when they were a passenger three or four times in their life, about operating on. This, sort of, feel good, reflexive response comes naturally to politicians, can in fact not only be much help but can be damaging to the problem.

The key in this instance especially is we need to rely on the local management, which the Coast Guard now is what’s called Area Security Committees which are chaired by the (captain?) of the port that bring in the private as well as the local stakeholders. They need an enormous amount of delegated authority to manage these incidences. But they also need enormous capacity for planning and management. That function is being done as a collateral duty by the (captain?) of the port who also has a very other busy day-to-day job and who used to do something before 09/11. So huge lift to basically bring stakeholders together, conduct meetings, do planning and scenarios. It’s a full time job. Maybe we should give more bodies to support this and play this quarter and plus a back-up capability at that local/regional level instead of trying to build the super ubercenter here in the federal government to manage the maritime industry overall. And those are also the value of that here in many cases, like especially in places like L.A. and Seattle/Tacoma, they assist the port relationships, they know the players in the industry and in Hong Kong, in Singapore, on the mainland in China, better than anybody in the U.S. government knows because they’re working with them on an ongoing basis. Any problem – just basic mechanics problems associated with trade puts them in regular contact, so they know who to pick up the phone and talk to. So when you delegate this down to these players you’re also actually getting, many times, an international dimension. But it’s resourcing it adequately for them to play this role, to do the planning, to do the real assessments about the areas and you got to look beyond the wharf. You have got to look, you know, at the energy linkages. You’ve got to look at the linkages of surface transportation – train and rail and so forth – and how all these pieces come together.

Again, that’s best done at the port level – port community level coordinating and (regionalized?). It is a much more decentralized approach than the one we are likely to take right now.

MR. CROWLEY: Antoine, come forward. Dennis Rochford from the Maritime Exchange for the Delaware River and Bay is here. Dennis, let me – let me turn the tables here. One of the components in Joe’s paper on the issue of sustainment is perhaps taking the – of the \$15 billion that currently – customs duties that come from goods that flow through our 361 ports designated maybe 3 to 5 percent of those customs duties to port security over the long term so that ultimately once we are able to raise the bar, we get to some mechanism for sustainment over the long term that is not dependent on annual appropriations.

I want to get your reaction to that. But sitting there as president of the MEDRB, how do you plan to sustain whatever – port security and operations – over the long term?

DENNIS ROCHFORD: Thank you P.J. Let me take 60 seconds to maybe elaborate on who I am and how I got here. I run a trade association on the Delaware River, the Maritime Exchange for the Delaware River and Bay. We’re like the chamber of commerce of the Delaware River, but we also have an operating role. We’re three states, public/private port authorities, containers, oil companies, breakbulk facilities, et cetera. And so we have what’s known as Maritime Online, which is basically an Internet based system that captures and disseminates vessel, cargo, and crew list information; makes it available to the port community for commercial purposes, for regulatory purposes, Coast Guard, Customs and Border Protection, security purposes.

We actually are one of several – like 15 or 25 – marine exchanges making this information available to the Office of Naval Intelligence. On 9/11, it’s my understanding that the Office of Naval Intelligence did not have a single source of all the commercial vessels coming into United States ports, which would be useful information to have along with other information. We are also one of three pilot projects in the United States working with the Transportation Security Administration to develop the transportation worker identification credential, which if you give me the privilege to make a few comments it will be my question to these two gentleman up here in terms of their view of that project. And we work along with Los Angeles, Long Beach and the state of Florida on that project.

To your point, first of all, when I read it in Joe’s speech on the train coming down today, that is a good idea. The \$15 or \$16 billion generated through customs tariffs and fees, basically generated through import and international trade, would be a good source of funds to be supportive of maritime security. I’m of the opinion, by the way, and you two gentlemen have mentioned this, I think the number one priority in terms of maritime security as we pursue a policy in the United States is people.

People in terms of Coast Guard billets, people in terms of Customs and Border Protection, and first and foremost placing those people overseas. To Captain Flynn’s comment that the captain of the port now has to run this committee in addition to everything else and all the other responsibilities is a very valid point and they do depend

on reservists who go off at the end of the fiscal year, so the number one responsibility is to get people out there.

I don't want to diminish port security grants. I think they're important. I think at the end of the day, they're not going to be sustained by federal dollars for the operating expenses, et cetera, et cetera. I think we need to make those investments along the lines of the matrix in your speech, et cetera – what you wrote today; your paper.

But I think the number one responsibility is to put more resources to those federal agencies to be able to do their job on the ground at the port of embarkation, which would also include the United States where you have (coast-wide?) shipping. So it's just not a matter of sending a bunch of Customs and Coast Guard people overseas; it's also a matter of making sure you have adequate resources here.

On the dollar end of it and what we have talked about briefly on the paper yesterday on the phone, I think at the end of the day you're going to have a port security fee. They're already talking about that in Washington. Various ports around the country are establishing fees. I think the first step in that process is to do what I like to refer to as a source of use of funds: how much money public and private is coming in the maritime security, who is providing it, what should the fee be in order to pay for, as I think Dr. Bouchard is saying, the (delta?) in terms of the security requirements imposed by the federal government for the good of the nation. But that fee needs to reflect the fact that the people in the supply chain, including the people that own the cargo who are really concerned about maritime security – how many dollars they have invested in that.

So I've rambled on here about a lot, and my question on the transportation worker identification card is, where do you see that project today? How vital is it to maritime security, as you see it, in the United States? And what do you see as we go forward on it?

DR. FLYNN: Well, let me just reinforce first that this funding issue – my quip has often been that the only transportation sector where the federal government is parasitic versus supportive is the maritime sector. That is, the fees that are collected from maritime activity goes into the general treasury versus everywhere else on our surface transportation, aviation, the money goes back into the industry. So I think shortsightedly, the ports – the American Association of Port Authorities after 09/11 – well, when MISA was first proposed said, “We don't want any fees,” because their experience has been fees are charged for the year later and the money goes back in the general treasury when the crisis is over. And they were seeing this is a cost that were basically due here because that – they've been burned before. I would argue the security problem is ongoing and the politics of that would have been a little more problematic so they cut off the potential funding source, but clearly this customs revenue source is one as well as a security fee, which is put the money you're taking from the port back into the port. It should be not rocket science for a maritime nation to do this.

On the TWIC issue, it's stalled. It's just absolutely stalled. And there is – mostly the issues are, of course, concerns about civil liberty questions, the union issues, and so

forth, lack of consensus amongst the community where they go. As I've heard from union folks as well as folks who are working this in more detail here, it's not great opposition to this. It's just that there is legitimate concerns that we'll be silly. As anybody who has had a misdemeanor in the last – can't work in a port.

Well, we are not going to have a trucking industry if we take this thing too far, all right. I mean there is – you know, people do get in trouble and they do need to come back in life and work. So the focus really has to be what is the job they are doing? Do they a lot of discretion? And then you want to make sure the integrity is there versus if they had virtually no discretion. I mean, it's a box; they have no idea what's in it and they pick it up and take it from A to B and they do it on an ongoing basis; well, you don't need to be a squeaky clean person necessarily to do that activity.

So – but that's level of drilling down is not being done yet. The conversation has not matured. It basically is just in stall. The value, of course, is basic situational awareness. We'd like to know who is in the port. I mean, it'd be kind of handy. And if they knew that you know what's in the port, that'd be kind of handy, particularly if you had some intelligence, which we don't have, but if you had it that would be helpful. But it's pretty straightforward that we need to have a more visibility about the players, both to sift who the good guys are that we don't have to worry about, and the bad guys.

But one thing I would just also highlight, though, is we've got to be very careful and I think – than we have been about not getting a sort of us-versus-them, particularly when we were talking longshoremen union labor kind of issues here. I mean, these are Americans and they're very patriotic Americans. It's their livelihood. They are the ones who are going to be blown up and nobody understands the port better and what the risks are better than the people who work that port. I just got – last month, I was in the port of LA in Long Beach and given a tour – a security tour by the head of the International Warehouse and Longshoreman Union. I've been in that port 10 times with various inspections with government officials. This was the most eye-opening of the tours, all right.

These folks know what their vulnerabilities are, they know what the issues are, and they are a part of the solution, not part of the problem. And we got to find a way in which this vetting takes place and we manage that process and capitalize on their knowledge and their patriotism.

MR. CROWLEY: Joe, when you were the – you'll have the last word here. But when you were the head of Naval Base, Norfolk, you were one of the co-authors of the concept of the Joint Harbor Operations Center and you were saying that you were deliberately bringing some of these players into the system because they – day-to-day they know the feel of the port and they know and can clearly identify where the anomalies are.

DR. BOUCHARD: In just five seconds of background, I was the commanding officer of Naval Station, Norfolk, on 9/11 and Hampton Roads, the port, did not have a

vessel traffic system. Basically, the private sector took care of that service for the Coast Guard, but that also meant it had no foundation for effective port security. So myself and the captain of the port teamed up to build a port security system. We didn't – no one told us to do it. Technically, we didn't have authority to do it and I reprogrammed Navy money – got into a little bit of trouble with comptrollers, but we built a harbor security system centered on a joint harbor operations center, which subsequently it was the model for the Sea Hawk down in Charleston if you've heard of that.

Senator Fritz Hollings got real upset one day. One of his staffers was there and told me, "How come Hampton Roads has a J-Hawk and we don't have anything?" Well

–

DR. FLYNN: They now do. (Laughter.)

DR. BOUCHARD: – we didn't wait for the federal government to solve our problem for us; we just did it. But one of the key concepts there was that everybody in the port needed to be integrated into the security system. That's pretty much a common sense idea now, but what we realized is that the Navy and the Coast Guard didn't have a good feel for the day-to-day tempo of the port; what the normal operations were.

That kind of very detailed familiarity, even intuition, you get from the fishermen, the tug boat captains, the longshoremen. They know what's normal and what's not normal. So there are critical early warning components, so we integrated them and that paid off. And that's absolutely critical and that's an element of partnership that needs to be encouraged. And I hope that as the Coast Guard's new sector command center approach at all the major ports gets implemented, that it will tap into that kind of very intimate familiarity with the normal day-to-day tempo of a port.

Back to the TWIC card, my impression is – and I can really only speak for one port, although I've taken part in meetings where other ports were present too – stakeholder meetings. And at one point there was an initiative to come up with a common port credential for the whole East Coast and several of the ports got together to discuss it. There was a lot of apprehension that the manner in which TWIC is implemented will really make it difficult; that it will be expensive, it will be cumbersome, that it will have a negative impact on trade and employment. So whether TWIC is good or bad depends on exactly how it's implemented.

And Stephen is much more familiar with where it stands than I am, but there's a lot of concern that the federal government won't do it right. One immediate impact that the pending implementation of TWIC is having is several ports would like to beef up their own credential systems. For example, in Hampton Roads, we would like to have a single identification badge for all – there's approximately 90 port facilities covered by MTSA. We would like to have one single ID badge for all of them. Very cost effective: rather than everybody having their own systems and redundant databases and on and on and on, if they could all team together and have one badge for the whole port, you save a lot of money.

And for people who operate on multiple terminals, they only have to carry one badge. You know, there are people now who have to have 20 badges hanging from their neck, which is silly. But implementation of that proposal is inhibited by TWIC because people don't want to make an investment in a port-wide badge only to have it superseded by TWIC.

Now, we may press ahead anyway. We've seen the TWIC standards that are being used in the prototype testing. I don't have a lot of confidence that TSA and DHS will stick to the standards they use for the prototype. I would fully expect that they'll come up with something totally different and that possibility is inhibiting a lot of local initiatives that would, (a), improve security and, (b), reduce their costs.

An alternative to a top-down federal TWIC program that might be more cost effective would be as long – as the federal government is willing to pay its fair share, would be to do like they did with state drivers licenses. Just set a uniform national standard: every port ID card has to meet the standard, just like they did for the state driver's licenses and then let the ports do it locally. But then help fund that because I guarantee you that the standard is going to be higher than the quality of most of those ID badges that facilities around the country are issuing. A lot more flexible. It eliminates some of the worst problems you could have with a national program being implemented poorly; achieves a lot more standardization. It would give a facility in Texas grounds for accepting a badge issued by a facility in Norfolk because it's – the card is the same standard and because it's the same standard, it's validity can be validated.

So there is an alternative to what is being proposed for TWIC now, although that approach maybe considered and I'm just not aware of it. But a lot of concern in the port industry about the direction TWIC will go.

MR. CROWLEY: And of course – a very quick question?

Q: I'm Skip Roberts with the Service Employees International Union. And I appreciated during your remarks hearing about the value of the human capital in the ports. We represent a lot of port authority employees from clerical and administrative (off mike) operations. One of the things, though, is while most of the threat will be waterborne on the ports, or at least that would be the anticipation, as the largest union of private security officers these are state regulated in 13 states. You could be hired today and be on the job tomorrow without even a criminal background check and we are fighting bottom-feeders in the industry to try and raise the standard. (Off mike.)

DR. FLYNN: Yeah, absolutely. I would take it a little bit further here. While I applaud very much the notion – a big advocate for the overseas dimension of it here. You know, the one major – the one terrorist incident we have involving a port in post-9/11 has been the Port of Ashdod in Israel where the terrorists came in a container with a false wall or bulkhead. The Israelis actually check empty containers when they come

into the terminals, but saw there was a wall there. These folks broke out and they were heading for one of the tank farms with suicide bombers.

They were intercepted by the Israelis. They killed eight Israelis and themselves in the process. But you can attack a port not just over there; we can attack them here. And checking what comes in – and that’s where this private security becomes also part of the process here, but if you’re going after a port it’s a lot easier to do it from here going into it because (unintelligible) the little bit of security in the port is all about stuff being stolen and leaving and it’s not of the monitoring what comes in. And so we really got to think about this again as a system. If that theme hopefully has come through and it’s there versus as a single beachhead that we – we turn into – with moats and walls, that’s just not going to work.

MR. CROWLEY: This is a very rich discussion. Obviously, we could take another hour and a half and still not cover the entire territory. A couple of quick thank yous to Anna Soellner and to Antoine Morris and our events team for helping to put on this. Please join me in thanking the two great panelists: Joe Bouchard, Steve Flynn. Thank you for coming.

(Applause.)

DR. FLYNN: Thank you.

DR. BOUCHARD: Thank you.

(END)