Press Office
U.S. Department of Homeland Security

Press Release

March 20, 2007
Contact: DHS Press Office, (202) 282-8010

REMARKS BY HOMELAND SECURITY SECRETARY MICHAEL CHERTOFF TO THE AMERICAN ASSOCIATION OF PORT AUTHORITIES

SECRETARY CHERTOFF: That was a great introduction, because it properly acknowledged what, in fact, my greatest accomplishment is: marrying up. (Laughter) I want to acknowledge Warren McCrimmon, the Chairman of the U.S. delegation, Allen Domaas, and also Kurt Nagle, who welcomed me here.

As I was listening to the invocation, I was desperately trying to figure how I was going to top the raising of the thing there. I tried to see if I could make the chandeliers shake or something. (Laughter.) That is a very tough act to follow, Father, very tough.

I appreciate the opportunity to be here with members of the American Association of Port Authorities, including those of you representing U.S. ports, and those of you from South and Central America, the Caribbean, and Canada.

We at the Department of Homeland Security appreciate your partnership, although we do have considerable authority when it comes to securing our ports, using our authorities in the Customs sphere and in the Coast Guard sphere. We don't actually own the ports, I'm sure you'll be pleased to hear, and we don't manage them. And that's good.

So it does have to be a partnership, when we talk about securing the ports. And, I want to thank you first for the tremendous cooperation that you have shown our department and our member agencies. I've had an opportunity to visit a number of the ports, and I'm always impressed by the close working relationship between our agencies and the people who have the responsibility for running the ports day to day.

Because of our collaboration, we've made significant advances since September 11th protecting our ports, and the billions of dollars of commerce that enter our country every year through the maritime domain. We've done this through new international maritime standards and security regulations, new technology and infrastructure improvements, and through new grant funding.

Of course, the port authorities, the terminal operators, and the port stakeholders have also made substantial investment, which reflects the fact that investments in security ultimately make good business sense.

Today, I would like to talk about three areas of port security that are critical areas for our department: first, keeping dangerous cargo out of the country and from entering our ports; second, strengthening the security of the infrastructure of our ports through the use of grant funding, as well as the work of the Coast Guard and Customs and Border Protection; and third, our plans for the Transportation Worker Identification Credential, which is designed to secure us against the possibility of infiltration from within.

Let me begin by discussing some key principles that apply to port security and, in fact, to all homeland security. First, we do not believe in security at any cost. We believe in risk management, which means looking at threats, vulnerabilities and consequences, weighing what are the risks we should be most concerned about, considering the measures we are looking to undertake, in terms of whether they are cost beneficial, and then weighing that in terms of making up a strategic plan.

We also believe in layered security. That's recognition of the fact that there's no magic bullet for security, whether it be our ports or elsewhere. Any single approach can fail. Therefore, the right answer is to build layers of security that build rings of protection. What that does is it counts on redundancy and on randomness as allies in building a total security network.

And this approach recognizes, of course, that ports themselves are part of a large network, a network that extends across the globe and requires us to measure security at every point from the element of manufacture, where you first take that which is going to be shipped and assemble it, all the way through to the ultimate delivery at the destination of the person who is receiving the consignment.

A third element of our strategy is to recognize that every port is different. A cookie-cutter approach to security will not work, and we don't want our security measures to do more harm than good. One of my favorite proposals is that which says we are derelict because we don't physically inspect every single container that comes into the country. How many here want us to do that? (Laughter) I guess I have my answer. We know that to do that would be to destroy the ports. We have to, in fact, use a risk-managed approach and a layered approach and a cost-beneficial approach to triage and select those elements of the container supply chain that we should take a close look at while letting the vast majority of flow go unimpeded.

Another area where we want to use common sense, for example, is the suggestion about doing all of our scanning for radiation overseas. That, again, is a very interesting proposal; it's one that in many places is a very good idea and we are working, as I'll explain shortly, to do that. But again, a cookie-cutter that says we must do it everywhere would fail to take account of our need to accommodate the requirements, legal and regulatory, of our foreign partners, as well as the fact that the footprint and architecture of ports are not identical. Ports with a lot of transshipment are much harder to do scanning in than ports with a large physical footprint where everything comes in through a central portal.

So, using all of these concepts, we have to apply a strategy to the objectives I've outlined to come up with a common-sense way to maximize port security, but always making sure that we are not damaging the system of maritime trade that we're trying to protect.

So, let me turn to the first of these elements of strategy: keeping dangerous cargo from entering the ports from the maritime side. How do we keep dangerous cargo from entering the ports? Well, first we have to extend our reach, and that's consistent with this approach of layered security. Our Container Security Initiative is now active in more than 50 overseas ports, accounting for 85 percent of container traffic bound for the United States. This includes nine CSI ports in the Western Hemisphere – ports in Canada, Brazil, Argentina, Honduras, the Dominican Republican, Jamaica and the Bahamas; and four more CSI ports will come online later this year in Colombia and Panama. This begins the process of inspection, in many cases, overseas before containers are loaded on a ship.

Our Secure Freight program is increasing the data we collect on containers that are going to transit the international supply chain. What that does is give us better information in order to select what containers we have to look at. And we are now testing the feasibility of overseas scanning for radiation to prevent the entry of WMD into our maritime domain. And again, that's the approach of trying as much as possible to move the scanning, where practicable, overseas at the earliest point at which containers enter the international freight domain.

As part of this effort to continue to extend our reach, we're working with six foreign ports, including Puerto Cortez in Honduras, to install radiation detection equipment to scan cargo for radiological and nuclear emissions. Construction began in Port Cortez in November, and operational testing will begin next month.

This program of overseas scanning has already exceeded the requirement of the Safe Ports Act to conduct 100 percent scanning of cargo in at least three foreign ports. And what it will do is test the viability of integrating this suite of scanning in some of the world's largest and most complicated port environments. What we learn during this first rollout is going to help inform everything we do as part of this general enlargement of our security envelope through the Secure Freight program.

Secure Freight is also, by the way, a great example of international cooperation, which is indispensable in securing the supply chain, because it can't work without the cooperation of multiple international actors.

We need to continue to work together to educate members of our own Congress on the nature and interdependence of the global supply chain, and to make sure that mandates that sound good as sound bites don't get imposed in a way that actually cripples the maritime trade, which is an engine of our very successful economy.

I also should point out though, that as part of our layered approach, we have built and enhanced our capabilities of scanning at our U.S. domestic ports, as well. In our own U.S. ports, which are ports that you all own and manage, we are now scanning more than 90 percent of the cargo for radiation, and we're going to reach 98 percent at our major seaports by the end of this year, and almost 100 percent for all ports of entry, sea and land, by the end of 2008. This is from the year 2000, where we scanned exactly zero percent. So that is a huge, huge revolution in our capability to protect this country from people smuggling in nuclear or radiological materials.

What about the port itself? Well, our principal vehicle for dealing with the ports is, of course, grants, which enable you to strengthen port infrastructure, and our expenditures in terms of the Coast Guard and Customs and Border Protection, and that equipment which we actually deploy at the ports. And I want to look at this holistically, because a lot of times I see stories in the paper that say, well, we spend billions of dollars on aviation, but we only spend millions on the ports.

That number undercounts the fact that our port security, while certainly grants are important to it, is not entirely dependent upon grants. A big amount of what we do to invest in port security is in-kind investment in the form of the Coast Guard –represented here by Admiral Allen, the Commandant – and Customs and Border Protection. If you were to take all of what we invest in port security over the last few years, you would see we've spent over $10 billion on port security.

The President's budget for fiscal year 2008 continues this very robust support for port security, including port security grants. We're requesting that Congress give us $210 million for port security, building upon more than $800 million in port security grants that has been distributed since 9/11, a total of over $1 billion. These grant funds are being used to build capabilities in and around port areas, covering the full spectrum of prevention, protection, response and recovery.

Let me give you some examples. We awarded the Port of New York over $77 million to secure facilities within its area, including $18 million to the Port Authority of New York and New Jersey to enhance surveillance capabilities and harden facilities against attack. We awarded the Port of Los Angeles in Long Beach, the largest container port in the U.S., over $91 million for similar work, including $8 million to build a new command and control center that will support federal, state and local security personnel with 24/7 surveillance capability.

And we've provided Washington State Ferries and the Staten Island Ferries $18 million, and $16 million, respectively, to fund physical enhancements to vessels and terminals, and increase monitoring capabilities.

This fiscal year, in which we're in the middle of distributing grants, we've released our grant guidance several months ahead of last year, and the majority of the grant funds we've already identified, $120 million, will be available to the eight, tier-one ports or port areas that we consider to be at the highest risk. This is consistent with our risk-based approach which looks at putting the most resources against those areas where threat, vulnerability and consequence give us the greatest risk.

As part of this, we've continually worked with stakeholders, including you, to refine and strengthen our risk analysis. We've placed greater emphasis on geographic risk, focusing on a regional approach so that we can cluster individual ports and analyze them as part of a single area, to reflect geographic proximity and the interdependency of assets, shared risk and shared waterway. That's an approach we've used, for example, up in northern California, and it's an approach we've used in Virginia in the Hampton Roads region. That's why 102 ports we identified as critical this year were clustered into 72

areas that align with our area maritime security strategies and our Coast Guard security operations.

And we continue to work with grant applicants to ask them to focus on key priorities and capabilities in the requests they make for money. We want to fund projects that increase awareness in and around port areas; address the significant threat posed by improvised explosive devices through USS Cole style attacks; expand training and exercises; implement the TWIC credential and access control process; and support our overall national preparedness priorities.

This year, more than ever, it's a collaborative process, and we want to continue to work with you to give the American taxpayer the most value for the taxpayer dollar.

So I've talked about keeping dangerous cargo out of the maritime domain, and protecting and strengthening the infrastructure. How do we prevent people coming within and posing a threat by masquerading as legitimate employees or service personnel? Well, we're doing that by developing the Transportation Worker Identification Credential, to make sure those who come into our ports are not a security risk, that they are authorized to do the work there, and that they are not using fraudulent or stolen credentials. TWIC will be a tamper-resistant, biometric credential for our nation's transportation workers, including port workers.

We estimate about three-quarters of a million port workers will be issued TWIC cards and that they will be required for all individuals who expect unescorted access to secure areas of MTSA-regulated facilities and vessels. TSA is responsible for conducting the security threat assessment on TWIC applicants, which includes a check against terrorist watch lists, an immigration status check, and an FBI fingerprint-based criminal history records check.

We issued the first set of regulations for TWIC in January, and the rule becomes effective in a matter of days, after which we expect to begin enrolling port workers. TWIC is going to have an immediate security benefit in terms of having a standard secure credential.

In successive months we'll be working on the more complicated issue of access control and use of TWIC readers. Many of you helped in developing the reader standard and will be involved in upcoming pilot tests. We will take what we learn from those tests and incorporate them into a second set of rule makings on access control requirements.

We recognize it's a complicated undertaking- it takes place in a demanding operational environment. But by taking this in stages: background checks first, credentials next, and then access readers third, we've been able to rapidly move forward while ensuring that we are carefully evaluating technology and operational impact at every step of the process.

Let me conclude by talking about an issue that perhaps stands outside of all of these, and that is the question of resiliency. As important as it is to protect ports, it is equally important to be resilient so we can resume operations if, in fact, an attack is successfully carried out. When we look at the experience of Hurricanes Katrina and Rita, we saw tremendous damage to the port structures, as well as all the pain and suffering and loss of

human life. Among other things, 1,800 aids to navigation were destroyed by the hurricanes, and the storm caused significant silting of the navigable waterways, and led to the sinking of 2,900 vessels in the region.

In order to make that recovery, one lesson out of Katrina is that planning is critical. In order to recover ports from the kind of damage we've seen in Katrina and Rita – and this is one of the lessons learned from those hurricanes – we have to plan ahead of time about how to resume operations. And that has to be a joint effort, one undertaken not only with the federal government, but with you who own the assets and employ the people who work in the ports.

Admiral Allen, who is here today, has made maritime disaster recovery one of his top priorities as Commandant of the Coast Guard. And, in August of last year, the Coast Guard held a national maritime recovery symposium to begin addressing resiliency issues with the industry on a large scale. This event was an important step for developing a national approach to recovery planning. We need to identify issues and develop alternative solutions for recovery of the marine transportation system after an incident, whether it be manmade or natural.

The Coast Guard and CBP are working on national protocols for the resumption of trade, as we speak. This process includes the input from multiple agencies, including the Department of Transportation, TSA, and the Department of Defense. The private sector also has a major role in this process, and will be included through the Maritime Sector Coordinating Council and other outreach efforts, through out National Response Plan, the National Infrastructure Protection Plan, and the Maritime Infrastructure Recovery Plan. This will be an important focus for all of us in the months ahead.

We have done a lot in partnership with you to protect our ports without sacrificing the mobility of goods and the people that make our ports work in the first place. But we have more to do. I appreciate all you've done both in the U.S. and across the Western Hemisphere to balance trade and security, protect our ports and maritime cargo, but doing so while ensuring continued prosperity. We will remain your steadfast partners in this balanced effort to increase security and enhance prosperity. And we look forward to working with you in the time to come.

Thank you very much. (Applause.)

###