TESTIMONY OF ASSISTANT SECRETARY STEWART BAKER
BEFORE THE COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES
MARCH 2, 2006

Mr. Chairman, Ranking Member Skelton, and Members of the Committee, I am pleased to be here today to help discuss the critically important issue of port security and help clarify any questions you have about DHS's role in the Committee on Foreign Investment in the United States (CFIUS) and both DHS's consideration of the Dubai Ports World (DP World) acquisition of the British-owned Peninsula and Oriental Steam Navigation Company (P&O) and P&O's wholly owned U.S. subsidiary, P.O. Ports North America, Inc.

As DHS's Assistant Secretary for Policy, Planning, and International Affairs, I play a key role both in DHS's ongoing efforts to continue to strengthen port security and the CFIUS process. As you know, I oversaw the DHS review of the CFIUS transaction involving DP World and P&O. Based on a thorough review, meetings with the company that began more than six weeks before the company filed for review, and the binding nature of an assurances agreement between DHS and the company to ensure security at U.S. ports, I fully stand behind the decision DHS made in January 2006 not to further investigate this transaction..

Developments in the DP World Case

Nevertheless, DP World has announced that it is requesting an additional review by CFIUS. According to press reports, the company is likely to file a request for CFIUS review this week and seek an additional 45 day review.

DHS, as one of 12 CFIUS agencies, will be a full and active participant in that review, and welcomes the opportunity to review the transaction anew. As I explain in more detail below, DHS will once again consult widely with its experts in the Department, including those at Coast Guard and Customs and Border Protection (CBP) who have primary responsibility for port and cargo security.

Before getting into the specifics of the DP World transaction, I would like to provide a general overview of DHS's participation in the CFIUS process.

Overview of DHS Participation in CFIUS

DHS is the newest member of CFIUS, added by Executive Order in 2003, after DHS was created. DHS has participated in the CFIUS process actively, and has placed a significant focus on nontraditional threats, as DHS has broad responsibility for protecting a wide variety of critical infrastructures. DHS is often joined in raising these concerns by our

partners at the Department of Justice and Department of Defense, and others. DHS is proud to work in close cooperation with these sister Cabinet agencies.

There are dozens of transactions in a year that require CFIUS review. In 2005, for example, CFIUS considered 65 discrete filings. DHS conducts a thorough review of each CFIUS case, and raises its concerns where issues arise.

The three most important questions DHS considers before deciding to seek an investigation are –

(1) Does DHS already have sufficient legal or regulatory authority to eliminate any threat to homeland security that might be raised by the transaction?

(2) Does DHS have homeland security concerns about the parties or nature of the transaction?

(3) If DHS has homeland security concerns, can they be resolved with binding assurances from the parties to the transaction?

Only after answering these questions does DHS decide whether to seek an investigation in CFIUS. DHS examined those questions in the DP World case and, as I will explain in more detail, made the judgment not to object to the transaction. All of the other 11 CFIUS member agencies made a similar decision after conducting their own independent reviews of the transaction.

DHS Legal Authority at the Ports

Congress has granted DHS sufficient legal authority to regulate the security of America's ports and the cargo that passes through each of those ports.

Under the Magnuson Act, the Ports and Waterways Safety Act, and, most recently, the Maritime Transportation Security Act of 2002 (MTSA), the U.S. Coast Guard has great authority to regulate security in all American ports. This includes the security for all facilities within a port, including terminal operators and vessels intending to call at a port or place subject to the jurisdiction of the U.S.

The Role of Terminal Operators like P&O and DP World

Let me first clarify what terminal operators do.

They do not run ports.

They certainly don't provide or oversee security for the entire port complex. That is the responsibility of the government and the local port authority, which is usually a government agency.

Terminal operators also do not obtain a comprehensive window into the breadth and depth of security measures that DHS employs to protect our ports and the cargo that

enters those ports. The public fears that the DP World transaction have generated on this point are misplaced and lack a firm factual foundation, as I will explain later.

Terminal operators ordinarily sign a long-term lease for waterfront property in the port. They build a pier for ships, cranes to unload the ship, a parking lot to store the containers they unload, and perhaps a small management office. They make their money lifting containers out of ships and holding them for shippers.

That's what we're talking about here. Through its acquisition of P&O, DP World is hoping to take over the leases at twenty-four terminals in the U.S. That's a relatively small part of the operations in the six ports where they would operate terminals, including New Orleans, Houston, Miami, Newark, Baltimore, and Philadelphia. Their filings indicate that DP World will also take over the P&O equities at other ports, but these consist of stevedoring and labor operations where P&O is not the designated terminal operator.

I understand from the Coast Guard that there are more than 800 regulated port facilities in the six ports where P&O operates terminals in the U.S. So the twenty-four terminals in question here constitute less than 5% of the facilities in those six ports.

MTSA requires each terminal operator - because they operate inside the port – to file a facilities security plan with the Coast Guard that specifically details their compliance with all of the security measures required by Federal law, including those enforced by the Coast Guard. The Coast Guard inspects the terminal and can check the terminal operator's plan at any time, and require more effective measures if the Coast Guard deems they are necessary.

These MTSA requirements for U.S. port security do not turn on the nationality of the terminal operator. U.S., British, Chinese, and UAE terminal operators are all subject to the same legal requirements, and the Coast Guard Captains of the Port can tailor each security plan to address the particular circumstances of each location.

Coast Guard Actions under MTSA

The Coast Guard has inspected and approved facility security plans for some 3,200 facilities regulated by MTSA. In addition, Coast Guard has completed Port Security Assessments and Port Threat Assessments for all 55 military and/or economically critical ports.

Forty-four Area Maritime Security Committees have been formally chartered and have developed Area Maritime Security Plans for the purpose of detecting, deterring, and preventing terrorist attacks as well as responding in the event of an incident. These committees are chaired by a local Coast Guard official, the designated Federal Maritime Security Coordinator, and include port authority, vessel, facility, labor interest as well as federal, state and local agencies.

The Coast Guard established an International Port Security Program to assess the effectiveness of anti-terrorism measures in place in overseas ports. Thirty-seven of the 44 countries assessed to date have substantially implemented the International Ship and Port Facility Security ("ISPS") Code. These 44 countries are responsible for over 80% of the maritime trade to the United States. The seven countries that are not in substantial compliance have been or will be notified shortly to take corrective actions or risk being placed on a Port Security Advisory and have Conditions of Entry imposed on vessels arriving from their ports.

The Coast Guard has conducted 16,000 foreign flag vessel boardings for security compliance with the ISPS Code since July 2004. These boardings were conducted either offshore or in port, depending on the risk assessment completed prior to each vessel's arrival in a U.S port.

DHS Role in Cargo Security

The Administration recognized after September 11 that more was needed to protect the United States from terrorist attack, and it immediately identified the vulnerability posed by the millions of cargo containers entering our ports each year. DHS plays a primary role in strengthening port and cargo security, and with the support of the Administration, we have made dramatic increases in these areas. Since September 11, funding for port and cargo security has increased by more than 700%, from $259 million in FY 2001 to $1.6 billion in FY 2005. This upward trend continues with $2 billion for DHS port security allocated in FY 2006, and an addition 35% increase to $2.8 billion in the President's Budget request for FY 2007.

This money has of course funding port security grants of more than $870 million. It has also built a layered security strategy that pushes our security measures overseas. The reason is simple. The Federal Government realized after the 9/11 attacks that it would be far better to detect and interdict a threat to the U.S. when that container was thousands of miles away, rather than sitting in a U.S. port. So we pushed our borders out to do much more inspection and screening of cargo before it ever arrives at our shores.

The 24-Hour Rule and CSI

Our authority over shipping containers begins even before the container is loaded in a foreign port – and long before that container arrives in the U.S. We require foreign companies to send us a list of the contents of a container 24 hours before the container is loaded on board the ship *in the foreign country.*

If Customs and Border Protection (CBP) concludes that the contents of a particular container may be high risk, we can have it physically inspected or x-rayed in cooperating foreign ports.

This program, known as the Container Security Initiative (CSI) depends on the voluntary cooperation of foreign governments and foreign companies. We've gotten that

cooperation around the world – including in Dubai, the United Arab Emirates. The CSI currently operates in 42 of the world's largest ports. By the end of this year, the number of cooperating ports is expected to grow to 50, covering approximately 82 percent of maritime containerized cargo shipped to the U.S.

Twenty-four hours before a ship is loaded, and therefore prior to departing the last foreign port for the United States, DHS receives a complete manifest of all the cargo that will be on that ship when it arrives in a U.S. port. This includes all cargo information at the bill of lading level, whether the cargo is destined for the U.S., or will remain on-board while in a U.S. port but destined for a foreign country. This rule applies to all containerized sea cargo whether departing from a CSI port or not.

Mandatory Advance Notice of Crew Members to DHS

Depending upon the length of the voyage, DHS receives additional notice concerning the crew of the vessel 24 to 96 hours before the vessel arrives in the U.S. This is full biographic data identifying the crewmembers and passengers, if any, so that DHS can screen them against risk indicators, the terrorist watch list and other databases.

We also get information from the importer describing the declared value and description of the goods being imported.

Risk Analysis of Cargo and Crew

Thus, long before a cargo ship arrives at any U.S. port, DHS has the shipper's information, the ship's information, and usually the buyer's information about what is in the container. The data is compared to ensure that it matches, and is also compared against historical information to detect anomalous patterns.

This data is all scrutinized and processed through a complex program that runs against hundreds of risk indicators to assign the ship and its cargo a risk score. The crew and passengers are all vetted prior to arrival.

DHS has full information about the vessel, its contents, and the people on-board.

If DHS has a concern about the cargo, the Coast Guard and CBP meet and decide an appropriate course of action, which may include boarding the vessel at sea or at the entrance to the ship channel, or meeting the vessel dockside and immediately inspecting the suspect containers.

Coast Guard has established a process to identify and target High Interest Vessels. This process has resulted in 3,400 at sea security boardings, and 1,500 positive vessel control escorts since 2004 to ensure that these vessels cannot be used as a potential weapon

What the Terminal Operator Knows about U.S. Security Measures

I noted earlier that ownership of a terminal operation does not give the terminal operator – foreign or domestic – a unique insight into the breadth and depth of DHS security measures nor provide a crafty terminal operator with ill intent access to inside information to avoid or evade DHS scrutiny.

The first time a terminal operator at a U.S. facility sees any of the law enforcement and security measures that DHS has in place concerning the vessel and cargo is when the ship arrives in the U.S. Even then, all the terminal operator knows is that CBP has selected certain containers for examination. The operator is simply instructed to unload the containers, under DHS supervision, and deliver them to CBP for inspection. They are not told why.

CBP Examines 100% of Risky Containers

As I have noted already, CBP screens 100% of containers for risk. All containers that DHS determines to be of risk are examined using a variety of technologies. These technologies include: radiation screening, non-intrusive x-ray inspection, and as appropriate, physical examination.

This screening and examination is carried out by DHS employees tasked with the security of our seaports. They are assisted by longshoreman and stevedores in moving the containers, and by local law-enforcement authorities and port police to ensure the security of the port facilities.

All a terminal operator knows is that a container has been selected for examination, but not why the container was selected. The inspections and radiation detections are performed by CBP, not by the operator. Security is provided by a variety of government programs, agencies, and local law enforcement officials, not the terminal operator.

Special Measures to Detect Radioactive Devices

DHS component agencies and the DHS Domestic Nuclear Detection Office have worked closely with the Department of Energy to deploy radiation detection technology at domestic and foreign seaports. The Department of Energy is providing technical support to Dubai Customs to install four Radiation Portal Monitors in their main port in June. Some of this equipment is specifically dedicated to “in-transit cargo” passing through the Dubai port on its way to places like the U.S.

In the United States, we have deployed 181 radiation portal monitors at seaports to date, which allows us to screen 37 percent of arriving international cargo, and that number will continue to grow through the remainder of this year and 2007. CBP also has the ability to use portable devices to detect the presence of radiation at additional facilities, and CBP has issued over 12,000 hand-held devices to its officers. The President’s FY 2007 budget requests $157 million to secure next-generation detection equipment at our ports of entry.

Since there is often confusion on this point, I want to restate it. CBP subjects 100% of all containers shipped to the U.S. to a risk assessment analysis and subjects 100% of any container over a certain risk threshold to further inspection.

In short, DHS already has a large number of measures in place relating to port and cargo security that are designed to ensure the security of our ports. These measures, and additional measures taken by local port authorities, greatly reduce the risks presented by the presence of any foreign terminal operator in a U.S. port.

CFIUS Review of the DP World Transaction

DHS always examines the backgrounds of parties to a CFIUS transaction, and we did so in this case. DHS agencies – the Coast Guard and CBP -- had previously worked with both DP World and its management and found them to be cooperative and professional. Demonstrating this is the fact that DP World met with senior officials of DHS and DOJ on October 31 – more than six weeks before they filed on December 16 and our review began on December 17, to provide confidential notice of their plans and begin answering questions. At the conclusion of this thorough review,

DP World

DP World has played an invaluable role in the establishment of the first foreign-port screening program that the U.S. started in the Middle East. That's because Dubai also volunteered to help in this innovative approach to security. DP World has voluntarily agreed to participate in screening of outbound cargo for nuclear material, and it has worked closely with CBP and the Dubai Customs Authority to target high-risk containers destined for the U.S. These screening programs could not have been successfully implemented without the cooperation of Dubai Port World.

P&O's Participation in the Customs-Trade Partnership Against Terrorism (C-TPAT)

British-based P&O, the owner of the U.S. facilities DP World is seeking to acquire, is and was a voluntary participant in CBP's Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT establishes voluntary best security practices for all parts of the supply chain, making it more difficult for a terrorist or terrorist sympathizer to introduce a weapon into a container being sent by a legitimate party to the U.S. DP World has committed to maintaining C-TPAT participation for all of the P&O ports subject to this acquisition.

C-TPAT covers a wide variety of security practices, from fences and lighting to requiring that member companies conduct background checks on their employees, maintain current employee lists, and require that employees display proper identification.

C-TPAT's criteria also address physical access controls, facility security, information technology security, container security, security awareness and training, personnel screening, and important business partner requirements. These business partner

requirements oblige C-TPAT members, like P&O, to conduct business with other C-TPAT members who have committed to the same enhanced security requirements established by the C-TPAT program.

In Newark, New Jersey, all eight of the carriers who use P&Os Port Newark Container Terminal are also members of C-TPAT which increases the overall security of the Newark facility.

The DP World CFIUS Transaction

As I noted towards the beginning of my testimony, DHS considers three important questions in any CFIUS transaction: (1) does DHS already have sufficient legal or regulatory authority to eliminate any threat to homeland security that might be raised by the transaction?; (2) does DHS have homeland security concerns about the parties or nature of the transaction?; and (3) if DHS has homeland security concerns, can they be resolved with binding assurances from the parties to the transaction?

I have addressed the first two of those questions, now let me turn to the third.

As part of its CFIUS review, DHS considers whether it should obtain any further commitments from the companies engaging in the transaction to protect homeland security. DHS has been aggressive in seeking such assurances as part of CFIUS reviews. The assurances are carefully tailored to the particular industry and transaction, as well as the national security risks that we have identified.

The Assurances Agreements

DHS had never required an assurances agreement before in the context of a terminal operator or a port. But after analyzing the facts, DHS decided that we should ask for and obtain binding assurances from both companies.

The companies agreed after discussions to provide a number of assurances, two of which are particularly important.

First, both parties agreed that they would maintain their level of participation and cooperation with the voluntary security programs that they had already joined. This means that, for these companies, and these companies alone, what was previously voluntary is now mandatory.

In the U.S., the parties are committed to maintaining the best security practices set out in C-TPAT. In Dubai, the parties are committed to continued cooperation in the screening of containers bound for the U.S., including the radiation screening discussed above.

Second, the parties agreed to an open book policy in the U.S. DHS is entitled to see any records the companies maintain about their operations in the United States -- without a subpoena and without a warrant. All DHS needs to provide to DP World is a written

request and we can see it all. DHS can also see any records in the U.S. of efforts to control operations of the U.S. facilities from abroad.

Because C-TPAT requires a participating company to keep a current record of its employees, including Social Security Number and date of birth, this open-book assurance also allows us to obtain up-to-date lists of employees, including any new employees. DHS will have sufficient information about DP World employees to run the names against terrorist watch lists, to do background checks of our own, or to conduct other investigations as necessary.

These agreements were negotiated and obtained during the 30-day period the transaction was under CFIUS review, and DHS conditioned its non-objection to the transaction on the execution of those agreements.

The Assurances Letters to DHS are Binding and Legally Enforceable

The assurances that DHS obtained from the companies are binding and legally enforceable, so that DHS and the U.S. Government could go into court to enforce them.

The companies also agreed in the assurances letters that DHS could reopen the case, which could lead to divestment by the foreign company if the representations the companies made to DHS turned out to be false or misleading.

DHS believes that DP World will adhere to both the letter and the spirit of the assurances letter, because the worst thing that can happen to a terminal operator's business is to lose the trust of the CBP officials who decide how much of that operator's cargo must be inspected every day. If we lose faith in the security and honesty of these parties, we will have to increase government scrutiny of the cargo they handle. That means more inspections and more delays for their customers.

And that is very bad for business.

That is why DHS is confident that the companies will work hard to continue to earn and retain our trust – and to fulfill their assurances -- every day.

Conclusion

In short, after examining this transaction with care, DHS concluded that: (1) we have legal authority to regulate the U.S. security practices of these parties, including the ability to assess the maritime threat and intervene, at the foreign port of origin or on the high-seas, before potentially problematic cargo arrives at a U.S. port to be serviced by the parties; (2) DP World's track record in cooperating with DHS on security practices is already very good; and (3) DHS obtained assurances that provide additional protection against any possible future change in the cooperative spirit we have seen so far and that allow us to do further checks on our own.

Based on all those factors, DHS concluded that it would not object to the CFIUS transaction or seek an additional 45-day investigation.

I would be pleased to answer any questions that you have.