TESTIMONY OF ASSISTANT SECRETARY STEWART BAKER
BEFORE THE HOUSE TRANSPORTATION AND INFRASTRUCTURE
COAST GUARD & MARITIME TRANSPORTATION SUBCOMMITTEE
U.S. HOUSE OF REPRESENTATIVES
MARCH 9, 2006

Mr. Chairman, Ranking Member Filner, and Members of the Committee: I am pleased to be here today to help discuss the critically important issue of port security.

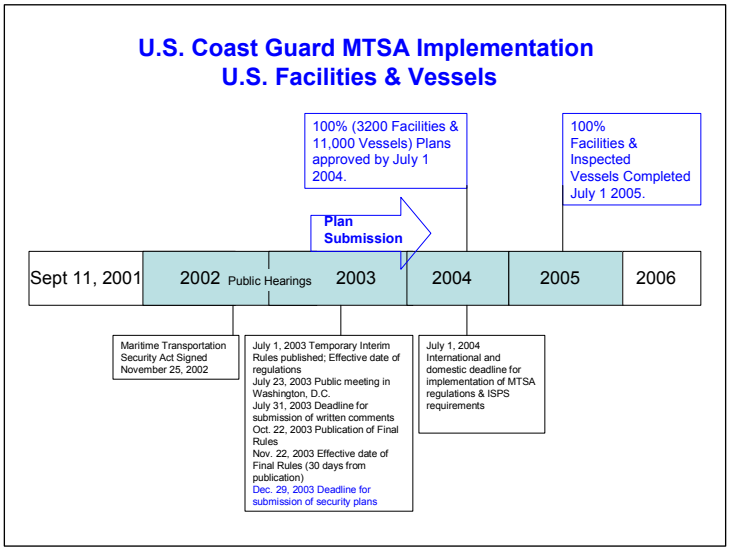
I am also available to help clarify any questions you have about DHS's role in the Committee on Foreign Investment in the United States (CFIUS) and DHS's consideration of the Dubai Ports World (DP World) acquisition of the British-owned Peninsula and Oriental Steam Navigation Company (P&O) and P&O's 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 in both DHS's ongoing efforts to continue to strengthen port security and DHS's participation in the CFIUS process.

DHS's Role in Ensuring Strong Port and Maritime Security

DHS continues to implement a multi-layered strategy to keep our ports safe and secure. Utilizing the expertise of our bureaus – particularly the United States Coast Guard and U.S. Customs and Border Protection – the private sector, and state and local authorities, we have made great strides since 9/11 to ensure that there are protective measures in place from one end of a sea-based journey to the other. With the President's FY 2007 Budget request, total DHS funding for port security activities since FY 2004 totals nearly $10 billion.

As the lead federal agency for maritime security, the Coast Guard routinely inspects and assesses the security of 3,200 regulated facilities in more than 360 U.S. ports at least annually in accordance with the Maritime Transportation and Security Act (MTSA) and the Ports and Waterways Safety Act (PWSA). Every MTSA-regulated U.S. port facility, regardless of the owner or operator, is required to establish and implement a comprehensive Facility Security Plan (FSP) that specifically addresses the vulnerabilities identified in the facility security assessment and details measures and procedures for controlling access to the facility, including screening, designating employees with key security responsibilities, verifying credentials of port workers,



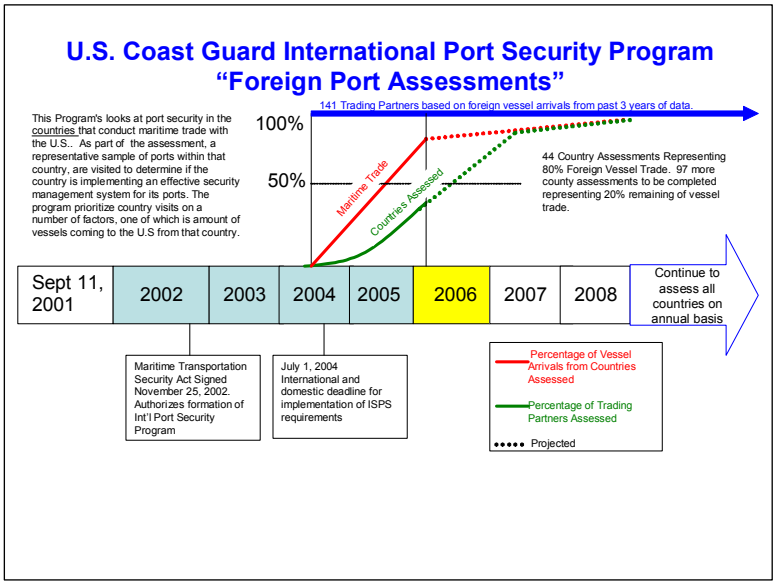
inspecting cargo for tampering, designating security responsibilities, quarterly training, drills and annual exercises, and reporting of all breaches of security or suspicious activity, among other security measures.

Working closely with local port authorities and law enforcement agencies, the Coast Guard regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance.

In accordance with MTSA, the Coast Guard has completed verification of security plans for U.S. ports and port facilities and vessels operating in U.S. waters. Specifically:

- Port Threat Assessments for all 55 militarily or economically critical ports have been completed. The Coast Guard has developed 44 Area Maritime Security Plans covering 361 ports, the Great Lakes, the Inland and Western Rivers and the Outer Continental Shelf region.
- The Coast Guard completed initial security plan verification exams on all 6,200 U.S. flag inspected vessels on July 1, 2005.
- The Coast Guard has completed 2,400 verification examinations on uninspected vessels regulated under the MTSA, and is on track to complete all 4,800 by December 31, 2006.
- The Coast Guard has reviewed and approved 3,200 facility security plans.
- The Coast Guard has approved 60 offshore facility security plans.

In addition to the Coast Guard's broad authorities for ensuring the security of U.S. port facilities and operations, the Coast Guard worked through the International Maritime Organization to develop the International Ship and Port Facility Security (ISPS) Code. Through the International Port Security Program, the Coast Guard has partnered with other nations worldwide to ensure compliance with the ISPS Code. The Coast Guard has assessed 44 countries, which are responsible for 80% of the maritime trade to the United States. Of those 44 countries, 37 have been found to be in substantial compliance with the ISPS Code. The seven countries that are not in substantial compliance have been or will soon be notified 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 is on track to assess approximately 36 countries per year.



The Coast Guard has also taken multiple steps to enhance our awareness in the maritime domain. The 96-hour Notice of Arrival regulation allows sufficient time to vet the crew, passengers, cargo and vessel information of all vessels prior to their entering the US from foreign ports. The Coast Guard also has expansive authority to exercise positive control over a vessel intending to enter a port or place subject to the jurisdiction of the United States. Since July 2004, the Coast Guard has boarded 16,000 foreign flag vessels for security compliance with the ISPS Code and the MTSA. Out of those 16,000 boardings, the Coast Guard imposed 143 detentions, expulsions or denials of entry. In addition, the Automatic Identification System (AIS) has been fielded at 9 ports with Vessel Traffic Service systems and allows the Coast Guard to identify and track vessels in the coastal environment. Long range tracking, currently in development, will enable the Coast Guard to identify and track vessels thousands of miles at sea, well before they reach our coastal zones. Likewise, the Inland River Vessel Movement Center provides critical information about the movement of hazardous cargoes along our Nation's inland rivers.

The Coast Guard has increased its operational presence through a number of other initiatives. For example, the Coast Guard has established processes to identify, target, and have conducted 3,400 security boardings on High Interest Vessels. These boardings included 1,500 positive control vessel escorts to ensure these vessels cannot be used as weapons of mass destruction. The Coast Guard has also established 12 Maritime Safety and Security Teams and enforced hundreds of fixed and moving security zones to protect Maritime Critical Infrastructure and Key Assets (MCI/KA) and Naval Vessel Protection Zones (NVPZ) to protect U.S. Navy and Maritime Administration vessels. Further, the Coast Guard is developing a Risk-Based Decision Making System, to be implemented this year, which will help prioritize High Capacity Passenger Vessels (HCPV) escorts. Although initially developed for high capacity ferries, its application is being expanded to enhance current security measures for other HCPVs: ferries, cruise ships, and excursion vessels carrying 500 or more passengers.

The Coast Guard is also working closely with various other agencies to implement the National Strategy for Maritime Security, and its eight supporting plans. Together, the plans provide the road map for the integration of national efforts in supporting the four primary pillars of maritime security: Awareness, Prevention, Protection, and Response and Recovery. As DHS's executive agent for implementing and updating plans related to Maritime Domain Awareness (Awareness), Global Maritime Intelligence Integration (Prevention), Maritime Transportation System Security (Protection), and Maritime Operational Threat Response (Response/Recovery), the Coast Guard, in cooperation with other stakeholders, is leading efforts to increase the coordination, effectiveness and efficiency of existing government-wide initiatives.

CBP Efforts Overseas Protect our Domestic Ports

In close coordination with the Coast Guard, the mission of the U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the United States by eliminating potential threats before they arrive at our borders and ports. For example, through a program administered by CBP, the Department has implemented the

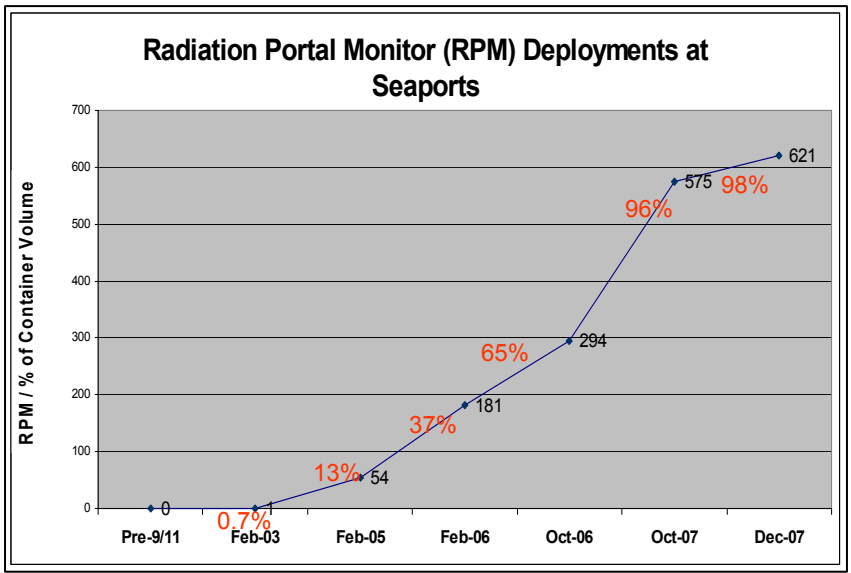
24-Hour Advanced Cargo Rule, requiring all sea carriers, with the exception of bulk carriers and approved break-bulk cargo, to provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port for shipment to the United States. Failure to meet the 24-Hour Advanced Cargo Rule results in a "do not load" message and other penalties. This program gives the Department greater awareness of what is being loaded onto ships bound for the United States and the advance information enables DHS to evaluate the terrorist risk from sea containers.

Similarly, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) initiatives bolster port security. Through CSI, CBP works with host government Customs Services to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States. In addition to the current 42 foreign ports participating in CSI, many more ports are in the planning stages. By the end of 2006, we expect that 50 ports, covering 82% of maritime containerized cargo shipped to the U.S., will participate in CSI. The table above shows the Department's substantial progress in expanding the CSI program since September 11, 2001.

Through C-TPAT, CBP has created a public-private and international partnership with nearly 5,800 businesses (over 10,000 have applied), including most of the largest U.S. importers. C-TPAT, CBP and partner companies are working together to improve baseline security standards for supply chain and container security. CBP reviews the security practices of not only the company shipping the goods, but also the companies that provided them with any services.

At present, the C-TPAT program has completed validations on 27 percent (1,545 validations completed) of the certified membership, up from 8 percent (403 validations completed) a year ago. Additionally, validations are in progress on another 39 percent (2,262 in progress) of certified members, and these validations will be completed throughout 2006, bringing the total percentage of certified members to 65 percent by years' end. In 2007, the C-TPAT program validations will continue. And we will have validated 100 percent by the end of CY 2007.

CBP also uses cutting-edge technology, including large-scale X-ray and gamma ray machines and radiation detection devices to screen cargo. Presently, CBP operates over 680 radiation portal monitors at our nation's ports, including 181 radiation portal monitors at seaports. CBP also utilizes over 170 large-scale non-intrusive inspection devices to examine cargo and has issued 12,400 hand-held radiation detection devices to its CBP officers. The President's FY 2007 budget requests $157



million to secure current and next-generation detection equipment at our ports of entry through the DHS Domestic Nuclear Detection Office (DNDO). Over 600 canine detection teams, capable of identifying narcotics, bulk currency, human beings, explosives, agricultural pests, and chemical weapons, are deployed at our ports of entry. As reflected in the Radiation Portal Monitor Deployment at Seaports table, 621 RPMs will be deployed to our Nation's top seaports, which will allow us to screen approximately 98 percent of inbound containers by December 2007.

CBP's National Targeting Center (NTC) is also a critical component of our layered port security efforts. The NTC provides tactical targeting and analytical research support for CBP anti-terrorism efforts. Experts in passenger and cargo targeting at the NTC operate around the clock using tools like the Automated Targeting System (ATS) to identify tactical targets and support intra-departmental and inter-agency anti-terrorist operations. The ATS serves as the premier tool for performing transactional risk assessments and evaluating potential national security risks posed by cargo and passengers arriving by sea, air, truck, and rail. Using pre-arrival information and input from the intelligence community, this rules-based system identifies high-risk targets before they arrive in the United States. The Department's Science & Technology Directorate (S&T) is supporting the introduction of advanced intelligent algorithms to further improve these risk assessment capabilities.

A key responsibility of the NTC is the support that it provides to the field, including tactical targeting and research support for the CSI personnel stationed at critical foreign ports throughout the world. The NTC, combined with CSI, C-TPAT, the 24-hour rule, and ATS ensures that all containers on-board vessels destined for the United States are risk scored using all available information; and that all cargo determined to be of high risk are examined. The NTC, working closely with the Coast Guard, also vets and risk scores all cargo and cruise-ship passengers and crew prior to arrival. This ensures that DHS has full port security awareness for international maritime activity.

Further, DNDO's FY 2007 budget request of nearly $536 million, a 70% increase from FY 2006, includes $157 million that will allow for the acquisition and deployment of nearly 300 current and next-generation radiation detection systems at our ports of entry. These systems will be deployed and operated by CBP. In addition, DNDO's FY 2007 budget also includes $30.3 million for the development of enhanced cargo radiography screening systems for our ports of entry. These enhanced screening efforts will compliment the many information-based programs the Department already has in place for enhanced port security.

In addition to increased screening efforts at our own ports of entry for radioactive and nuclear materials, the Department fully endorses the concept of increased active and passive detection at foreign ports of departure. The systems DNDO are acquiring and developing can also be used by foreign ports with a CSI presence, as well as the Department of Energy's Megaports program. We must continue to stress the need for increased screening at foreign ports of departure, while at the same time have a robust screening effort at our own ports of entry.

In order for the Department to increase its visibility into the security of our international supply chains, S&T is developing technology solutions that can be applied across the supply chain. Part of this effort is the development of a new class of security devices that will monitor the integrity of intermodal shipping containers and enable CBP Officers, CSI personnel and the NTC to gather information on the status of a container to improve risk assessment and data collection. When coupled with the broad supply chain security architectural framework currently under development by S&T, the Department will have the capability to bridge data and information between container security devices, shippers, and the National Targeting Center (NTC).

Finally, in addition to the work of the Coast Guard, CBP, S&T and the DNDO, the Port Security Grant program has awarded over $700 million to owners and operators of ports, terminals, U.S. inspected passenger vessels and ferries, as well as port authorities and State and local agencies to improve security for operators and passengers through physical security enhancements. The mission of the Port Security Grant program is to create a sustainable, risk-based effort for the protection of ports from terrorism, especially explosives and non-conventional threats that would cause major disruption to commerce and significant loss of life.

The Preparedness Directorate will announce the application process for an additional $168 million in port security grants in the coming weeks, bringing total funding to over $870 million since 9/11. In addition, the FY 2007 President's Budget bolsters funding for infrastructure protection, including ports, through the $600 million Targeted Infrastructure Protection grant program. The FY 2007 request consolidates existing infrastructure grant programs into a single program with a 55 percent increase in funding.

With all of the layered efforts already in place, and the ongoing efforts that are supported in the 2007 budget request, port security has substantially improved since 9/11, and since the creation of the Department of Homeland Security.

DHS Legal Authority at the Ports

Congress has granted DHS legal authorities to take steps to ensure 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 MTSA, the U.S. Coast Guard has 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.

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 $2.164 billion in FY 2004 and $2.183 billion in FY 2005. This upward trend continues with $2.455 billion for DHS port security allocated in FY 2006, and an additional 35% increase to $3.172 billion in the President's Budget request for FY 2007.

This money has helped implement 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 United States 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 United States. 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 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.

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 United States. 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 manifest 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.

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

There has been a lot of attention in recent weeks about the potential threats posed by terminal operators. 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 United States. 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 a 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 United States. 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.

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 United States. 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 DHS' DNDO 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 allow us to scan 37 percent of arriving international cargo, and that number will continue to grow through the remainder of this year and 2007—again, allowing us by December 2007 to scan 98 percent of inbound cargo . 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 with more on the way.

Since there is often confusion on this point, I want to restate it. CBP subjects 100% of all containers shipped to the United States 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.

The DP World CFIUS Case

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 stand fully behind the decision DHS made in January 2006 not to request further investigate this transaction.

Developments in the DP World Case

Nevertheless, DP World has announced that it is requesting an additional review by CFIUS. As noted by press reports, the company recently filed a second request for CFIUS 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. While we believe the 30-day review was rigorous and thorough, DHS will not prejudge its recommendation as a result of this 45-day investigation. DHS will also consider and investigate any additional steps the company proposes as part of its new notification or actions that it commits to taking, as well as any information provided by state or local officials or by members of Congress. 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.

CFIUS reviews dozens of transactions each year. 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 resolve 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, based on this careful assessment, made the judgment not to object to the transaction. All of the other 11 CFIUS member agencies conducted their own independent reviews of the transaction.

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 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.

DP World

DP World has played an invaluable role in the establishment of the first foreign-port screening program that the United States 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 United States. These screening programs could not have been successfully implemented without the cooperation of Dubai Ports 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 United States. 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 previously noted, DHS considers three important questions in any CFIUS transaction: (1) does DHS already have sufficient legal or regulatory authority to resolve 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 CFIUS review relating to 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 to ensure that the companies would continue their record of cooperation with DHS.

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 United States. 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 United States 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 commitments 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 an exchange of letters memorializing those commitments.

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.