After the Dubai Deal: International Trade and Cargo Security
Forum hosted by Senator Max Baucus
Ranking Member, Senate Finance Committee
April 3, 2006

Joseph F. Bouchard, Ph.D.
Executive Director
Center for Homeland Security and Defense

Lessons Learned from the Dubai Ports World Controversy

This forum is timely and important because the concept of partnership with industry has been called into question by the Dubai Ports World controversy. The reality that was overlooked in the outcry is that there already is extensive foreign ownership in the maritime terminal operations and shipping industries.

This extensive foreign ownership means that banning or severely restricting foreign investment, as has been proposed in at least a dozen bills introduced in the Congress since February, is not a viable option. Doing so would have severe negative economic consequences for the US. Additionally, it would not enhance US homeland security. Any US company that operates overseas can be exploited by terrorists to attack the United States just as easily as a foreign company that operates in the United States.

We face a fundamental strategic choice: Treat the private sector as part of the problem or part of the solution. If we choose to treat the private sector as part of the problem, we are saying that it cannot be trusted to implement effective security measures and must be treated with suspicion as potential threats to US security. The implication is astronomically greater security costs for the US government and loss of invaluable, irreplaceable insight and expertise of private sector. Additionally, the security measures that would have to be put in place could seriously disrupt the flow of international trade with little or no appreciable in crease in US homeland security.

If we choose to treat the private sector as part of the solution, we recognize that US importers, their overseas suppliers and the shipping industry have a vested interest in effective security, can be a reliable partner, offers awareness of potential threats not available from other sources. The US Government has chosen partnership, treating industry part of the solution – this is the only effective strategy and the partnership strategy must encompass foreign companies.

The most significant negative consequence of the outcry over foreign ownership the maritime terminal operations industry is that it diverts attention from serious weaknesses in US port and cargo security efforts. The proper response – and only effective response – to this belated recognition of the reality of foreign ownership in the maritime terminal operations (MTO) and shipping industries is to correct the weaknesses in current US supply chain security efforts.

Requirements for Effective Supply Chain Security

Effective cargo security requires effective security measures be in place across the entire supply chain, from the overseas factory where the good to be shipped are packaged and crated, all the way to the recipient of that shipment in the United States. Viewed from this perspective, cargo security requires much more than better seals on containers and better tools for screening and

inspecting cargo – it requires a set of mutually supporting initiatives designed to defeat every tactic terrorists may try to use to smuggle their contraband into the United States.

Effective supply chain security thus requires:

- Intelligence: Supply chain security requires intelligence efforts looking for and analyzing the right information, and rapid, unconstrained inter-agency information sharing. No individual US intelligence agency is omniscient: information that may be meaningless to one agency may be vital for another agency.
- Immigration: Supply chain security requires an effective US-VISIT program and effective means of identifying suspected terrorists attempting to enter the United States.
- Credentialing: Supply chain security requires implementation of the Transportation Workers Identification Credential (TWIC) with appropriate background checks, and effective access control to sensitive port areas and shipping data.
- Cargo security: Supply chain security requires effective screening of all cargo destined for the United States, including an Automated Targeting System (ATS) that provides very high probability of detecting smuggling, the capacity to conduct inspections of a sufficient amount of the cargo destined for or entering the United States to have confidence that it does not contain terrorist contraband, including a mix of non-intrusive inspection (NII) equipment employed in a manner that recognizes its inherent limitations and physical inspection (opening and unpacking containers), the Container Security Initiative (CSI), and the Customs-Trade Partnership Against Terrorism, (C-TPAT).
- Port and vessel security: Supply chain security requires effective implementation of the Maritime Transportation Security Act (MTSA) by US port authorities and private sector owners and operators of port facilities and vessels, as well as the efforts of the US Coast Guard, other Federal agencies, and state and local law enforcement.

Second, effective supply chain security requires strong international cooperation – working with the International Maritime Organization (IMO) on the International Ship and Port Security (ISPS) Code, with the International Labor Organization (ILO) implementation of the Seafarer Credential, and with the World Customs Organization (WCO) on international standards for supply chain security, including shipping documents, reporting and sharing of shipping data, and standards for screening and inspecting cargo. Cooperation with many other international and regional organizations, such as the European Union, is vital as well.

Third, our trading partners must have effective supply chain security programs. That requires effective, sustained implementation of the international programs just described and close cooperation between their agencies responsible for supply chain security and their US agency counterparts, such as CBP, the Coast Guard and the FBI.

Fourth, effective supply chain security requires close partnership with the maritime terminal operations and shipping industries – US and foreign.

Enhancing Supply Chain Security

Although improvements are needed across all of the areas related to supply chain security mentioned above, I will focus on four specific areas of weakness: cargo inspections, cargo screening and C-TPAT.

Cargo screening. The DHS and CBP strategy for cargo security is to rely on screening of all cargo destined for the United States in order to determine which shipments should be inspected. Because only a small percentage of cargo is inspected, the effectiveness of this strategy and the security of the United States depend upon how well ATS performs.

Although DHS and CBP frequently express confidence in ATS, there are reasons for concern. First, GAO has repeatedly identified weaknesses in ATS, some of which CBP has corrected on its own initiative but others have required Congressional action to compel action. Second, there is anecdotal evidence based on press reports of illegal narcotics having been found in cargo cleared by CBP that at least some drug smugglers have figured out how to defeat ATS. Third, the shipping industry and cargo security experts have been warning for years that the data used by ATS is not sufficient to detect smuggling. ATS only looks at the bill of lading (cargo manifest, a list of all the items in a shipping container) for any indications that a shipment may contain contraband. Although CBP claims that information from the intelligence community is also input into ATS to identify threats, that intelligence information can only be crossed with the extremely limited and easily forged information in the bill of lading.

CBP has tacitly acknowledged this weakness by launching a number of efforts to increase the amount of data it has on cargo shipments in order to detect indications of smuggling at any point in the supply chain, not just in the bill of lading presented to CBP when the shipment is manifested for a US port. The shipping industry has put forward a number of valuable proposals for increasing the data on cargo shipments available to CBP for cargo screening and shared them with DHS via the Committee on Commercial Operations of Customs and Border Protection (COAC). In 2005 DHS announced that the Secure Freight Initiative would be the means of increasing the cargo shipment data available to CBP for cargo screening. Although the Secure Freight Initiative appears to be an excellent concept, little progress has been made in implementing it. Congress should direct DHS to make timely and effective implementation of the Secure Freight Initiative, in partnership with the shipping industry, one of the department's top priorities.

Cargo inspections. The fact that CBP only inspects a small percentage of the cargo entering the United States, estimated to be only about four to six percent, has resulted in calls for 100% of all cargo to be inspected. The reality is that it would be impossible to conduct physical inspection of all cargo entering the United States. In 2005 approximately 11 million loaded shipping containers entered the United States. The manpower requirements alone make opening and unpacking all of those containers unrealistic. More importantly, the delays in cargo flow that would result from 100% physical inspection would cause severe damage to the US economy.

Some advocates of 100% inspection claim that non-intrusive inspection equipment is the solution. Such claims must be viewed with great skepticism. Although non-intrusive inspection equipment has a vital role to play in overall US supply chain security efforts, it is not a panacea. The equipment has serious limitations that can be exploited by terrorists seeking to smuggle contraband into the United States. Although DHS has on-going research and development efforts to develop better non-intrusive inspection equipment, even the best equipment money can buy would still have inherent limitations that prevent it being the sole solution for supply chain security.

Deployment of non-intrusive inspection equipment overseas to inspect cargo before it is loaded on a ship bound for the United States may be a great idea in theory, but is problematic in

practice. Without stringent safeguards to ensure that the equipment is operated properly and terrorists cannot evade having their shipments intercepted, non-intrusive inspection equipment overseas is worthless. Thus, excessive reliance on non-intrusive inspection equipment would thus give us a false sense of security while inadvertently increasing our vulnerability.

Two additional concerns about non-intrusive inspection equipment must be addressed. First, despite claims that use of non-intrusive inspection equipment for 100% inspections will not cause significant delays in cargo movement through ports, those claims have not been proven in real world operations. Limited experience to date strongly suggests that 100% inspections would cause delays, which could be unacceptable in an era of "just in time delivery." Better understanding of the impact of 100% non-intrusive inspections is needed before committing to a specific approach or large-scale procurement of non-intrusive inspection equipment. Finally, non-intrusive inspection equipment is extremely expensive to purchase, maintain and operate. Given the inherent limitations of non-intrusive inspection equipment, a prudent risk management approach to homeland security requires that investments in such equipment be balanced against the need for investments in other areas.

To return to the original issue – concern that only a small percentage of cargo entering the United States is inspected – the real issue is not what percentage is being inspected. Rather, the real issue is whether or not all the cargo that should be considered suspect is being inspected, and inspected in the right way. This has three implications. First, ATS had better be extremely good at identifying suspect containers. As described above, this is an area of concern that needs to be addressed as a matter of priority.

Second, CBP must have the capacity to inspect all of the containers flagged by ATS as suspect – and do so in a timely manner that does not unnecessarily impede the flow of cargo. Conversely, it would be unacceptable for CBP to in any way constrain the number of containers flagged by ATS based on the number that CBP has the capacity to inspect. Doing so would be a flagrant violation of the risk management principles on which the entire US cargo security strategy is based.

Third, suspect containers must be inspected in the right way. Obviously, it does no good to scan a container suspected of containing conventional explosives with radiation detection equipment; but it can be equally unproductive to scan the container with imaging equipment (like x-ray machines) if the density of the explosives is similar to the density of the legitimate cargo. The DHS investment strategy for non-intrusive inspection equipment and other sensor systems must strike a balance between different technologies best suited for detecting different types of threat contraband, taking into account risk management principles such as the likelihood of different threat materials being smuggled (such as conventional explosives versus radioactive material).

C-TPAT. C-TPAT is an excellent program that has the potential to make a significant contribution to supply chain security once its current weaknesses are corrected. Much to its credit, CBP has been selectively raising C-TPAT security standards when appropriate to do so. Examples of additional measure that would strengthen C-TPAT include:

- Accelerate the rate at which initial certification inspections are being conducted to eliminate the backlog of inspections by the end of Fiscal Year 2007.
- Require completion of certification inspections before a company is granted C-TPAT certification from October 1, 2007 onward.

- Implement a program of on-going C-TPAT compliance spot checks of certified companies, with no less than 20% being spot checked each year.
- Require foreign companies seeking C-TPAT certification to ship all their cargo through CSI ports.
- When the Secure Freight Initiative in implemented, make participation in it a requirement for C-TPAT certification.
- Establish standards for the quality and timeliness of cargo manifest submission. Companies that exceed a specified error rate or late submission rate have their C-TPAT certification suspended until they meet CBP standards.
- Establish a "no fault" reporting system for C-TPAT certified companies to report security lapses that CBP may need to factor into its automated targeting of containers for inspection.

Another important approach for correcting the weaknesses in C-TPAT, some of which are inherent in a voluntary program, is to integrate C-TPAT with complementary programs that compensate for its weaknesses. A serious limitation of current US supply chain security efforts is insufficient integration across the various security programs mentioned above. Although information sharing across the agencies responsible for those programs has increased significantly, the US government still does not have an overarching framework for supply chain security that enables the various programs to work in concert. The key to success is to move beyond passive information sharing to polices that specify cause and effect relationships – actions that must be taken when indications of security lapses or terrorist efforts to exploit the shipping system for smuggling are detected.

A few examples of integrating across complementary programs:

- Within the Coast Guard: link MTSA compliance inspections in the US with ISPS compliance inspections overseas conducted under the International Port Security Program. Discrepancies at a marine terminal in the United States could be indicative of company-wide management problems that could cause security lapses at their overseas marine as well – and vice versa.
- Within CBP: link customs and law enforcement efforts in the United States and CSI efforts in foreign ports with C-TPAT – using information from those efforts to better identify vulnerabilities in particular C-TPAT participants that need to be corrected (perhaps suspending C-TPAT certification until they are corrected) and possibly weaknesses in the C-TPAT program itself that could be corrected by revising eligibility and validation requirements.
- Link Coast Guard port security efforts with CBP supply chain security efforts: Use Coast Guard MTSA and ISPS inspections to support C-TPAT and CSI, and feed into ATS. Use CBP agents stationed in foreign ports as part of CSI to spot ISPS compliance issues in between Coast Guard inspections. Use Coast Guard personnel experienced in ISPS compliance inspections to enhance C-TPAT validation inspections of foreign marine terminals and shipping companies that operate vessels. Conversely, C-TPAT validation inspections could help identify marine terminals in the United States and overseas that need greater Coast Guard scrutiny.

C-TPAT is particularly weak at preventing terrorist insiders in legitimate and totally innocent companies engaged in international shipping (including suppliers from whom shipments originate) from being able to circumvent US anti-smuggling programs. There are two types of insiders. The first is a terrorist operative that infiltrates a company by being hired by it. C-TPAT contains provisions to prevent this by requiring companies to conduct background checks on their employees, but CBP has no means of validating these checks or ensuring that they are being performed on an on-going basis. The other type of insider is the sympathizer: an ordinary citizen with no connections to any terrorist group, but who holds strong anti-American or anti-Western feelings and thus may be susceptible to a request to aid a terrorist group. The C-TPAT background check requirement is totally ineffective against the sympathizer threat if the employee has no known links to terrorist organizations at the time he or she is hired.

CBP should test two potential solutions to the insider problem:

- Require "two person integrity" in the creation and modification of shipping documents. At least two persons are required: one to create a document or change it and a second to validate the legitimacy of the document before it is entered into the shipping data system. This would prevent a single person in any company, from origin to destination, can forge a shipping document to disguise a terrorist shipment. A terrorist group would need two insiders to successfully forge shipping documents, which greatly complicates their efforts and increases the probability of detecting the effort (a conspiracy is easier to detect than a lone wolf).

- Require "end-to-end" audits of all shipments and preservation of all versions of shipping documents and changes to them – in other words, a documented chain of custody for a shipment that can be audited to detect unauthorized changes to shipping documents or a shipment that did not originate at the alleged originating company. The "Chain of Custody Document" recommended by the National Customs Brokers and Forwarders Association of America (NCBFAA) and the cargo shipment data elements recommended by the World Shipping Council would be a good starting point for defining the content of an "end-to-end" audit. An "end-to-end" audit would validate the legitimacy of a shipment from originator to recipient, including any company that had a role in shipping it in between, and would be required whenever a shipment changes transportation mode (such as being loaded on a ship or transferred from one ship to another at a transshipment port) or crosses a national border (enters or leaves a country). If the shipping document for a shipment destined for or entering a US port does not match the shipping records at the company of origin or the destination company, it would be flagged for inspection. Any changes to shipping documents that did not match similar changes in the documentation or records of the rest of the chain would also flag the shipment for inspection. Such "end-to-end" audits would require terrorists to make a massive effort to penetrate a number of companies in order to ensure that a shipment containing contraband is not detected by CBP.

A first step toward implementing these two measures would be to make two person integrity and supplying data needed for end-to-end audits requirements for C-TPAT certification, at least for the highest level of benefits. This in turn would be a pilot project for developing a manageable

system for implementing these requirements internationally via the World Customs Organization (WCO).

Maritime Transportation System Resiliency

Maritime transportation system resiliency means effective measures to minimize the disruption of maritime transportation caused by a security incident and the ability to rapidly restore the maritime transportation system to full capacity. Resiliency requires four things: focused security response plans, cargo flow management, consequence reduction, private sector risk management, and recovery plans and capabilities.

Focused security response plans. Effective plans for managing the security response to a terrorist incident (or indications of an imminent terrorist threat) involving some element of the maritime transportation system. Simply shutting down the entire system would cause tremendous loss to the US economy, greatly amplifying the impact of the original event. US policy should emphasize isolating the impact of a terrorist attack on the maritime transportation system, using all available sources of information to determine if it is a stand-alone incident or one of multiple attacks, and implementing selective measures focused on countering specific threats. The security response should be as narrowly focused as possible, addressing the specific threat related vulnerabilities. For example, detecting a suspected radiological dispersal device ("dirty bomb") in a shipping container should not be grounds for halting oil tankers from entering unaffected ports. Nor should the entire intermodal shipping system be shut down. The response should be to identify a specific set of containers that should be treated as suspect based on everything that can be learned about the shipment that was intercepted. That set may be very large initially, but can be reduced as more information comes to light.

Cargo flow management. Cargo flow management means procedures for rapidly shifting cargo flows from terminals or routes that have been disrupted or are likely to be threatened would greatly reduce the impact of protective responses. To a large degree the shipping system is self-synchronizing and shippers will immediately begin making plans to divert vessels and cargo to other ports in the event of a terrorist incident disrupting maritime transportation through a port. Other than controlling diversion of Federally-chartered private vessels, the Federal Government should not attempt to directly control this process; it has neither the knowledge nor the resources to do so effectively. The Federal role should be threefold: (a) inform the private sector of restrictions at other ports so they do not attempt to divert cargo to them; (b) receive reports from the private sector and port authorities on ship diversion plans so the impact on Coast Guard and CBP resources in those ports can be assessed, and (c) if necessary, setting priorities for vessel movements based on their importance to the US economy and national security.

Port authorities and private facility operators will be monitoring the impact of diversions on their capacity and communicating this to the private sector. They should share this information with DHS to help the Coast Guard and CBP with management of their resources. DHS should also share this broadly with all fifty states because diversions will impact truck and rail traffic volume, and State agencies may have to adapt to prevent bottlenecks that impede restoration of cargo flows. State governments, in response, should inform their port authorities and DHS of land transportation restrictions (such as highway construction) that would limit the ability of a particular port to support increased cargo volume, and may need to consider suspending certain construction projects that would reduce traffic flow. (In some emergencies the U.S. Department of Transportation may even need to reprogram highway construction funds to rapidly complete a

project urgently needed to minimize disruption of cargo flow.) This approach will allow Federal agencies to focus their attention on the specific actions they can take that will have greatest benefit for maritime transportation system continuity of operations.

The most important capacity assessment that Coast Guard Captains of the Port and CBP Port Directors need to make is the capacity of Federal resources in unaffected ports to support increased vessel and cargo volume. They will need to rapidly determine the increased Coast Guard and CBP resources – personnel and equipment – that would be needed if vessel and cargo volume reached the peak capacity at specific unaffected ports. The Coast Guard probably would need to shift personnel and small craft to increase their capacity to conduct ship boardings and inspections, as well as to provide security for the increased vessel flow, and CBP probably would need to shift agents and non-intrusive inspection equipment to increase their capacity for container inspections, and immigration control (particularly if passenger vessels must be diverted). The Coast Guard and CBP should develop a standard methodology for rapidly conducting these resource assessments, develop a system for Captains of the Port and CBP Port Directors to request additional resources, and develop a national "triage" system for reallocating Coast Guard and CBP resources among multiple ports experiencing volume increases to meet national priorities.

In some incidents resource limitations may force the Coast Guard and CBP to set priorities for vessel movements based on their importance to the US economy and national security. For example, cruise ship movements may have to be suspended temporarily so that adequate protection can be provided for oil tankers.

Consequence reduction. Consequence reduction means measures that reduce the likelihood of an attack producing mass casualties or grave economic loss. For many high-risk port facilities, we achieve a greater return on investment from consequence reduction than from enhanced security measures. For example, if a terrorist attack is intended to cause severe economic loss by shutting down a critical marine terminal (such as an oil terminal) or even an entire port, but fails to do so as a result of prudent consequence reduction measures, then we have successfully prevent the terrorists from achieving their goal. Consequence reduction measures make sense from a business perspective as well as from a homeland security perspective. Minimizing damage and economic loss is a good investment for the owners of transportation facilities.

Consequence reduction focuses on safety, reliability and disaster prevention measures already covered in laws and regulations addressing safety and environmental protection. The Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA) have an important role to play in US homeland security efforts. For example, double hull tankers are required to reduce the likelihood of an oil spill in an accident, but also reduce the likelihood of an oil spill as a result of a terrorist attack. Similarly, oil pollution prevention and response regulations enforced by EPA and the Coast Guard contribute to reducing the consequences of a terrorist attack on a waterfront petrochemical terminal. The weakness in current laws and policies is that they are designed to prevent or mitigate the consequences of accidents or natural disasters and in many cases may not be adequate for the magnitude of damage that can be caused by a terrorist attack.

Private Sector Risk Management. Maritime transportation system resilience requires that private sector owners and operators of high-risk maritime transportation facilities have robust

risk management, emergency preparedness and continuity of business plans and capabilities. Such measures can significantly reduce the consequences of a terrorist attack, mitigating both their individual losses and the overall loss to the U.S. economy. Emergency preparedness and continuity of business make sense from a business perspective, can help reduce insurance costs, and are valuable for a wide range of emergencies, including natural disasters and major accidents as well as terrorist acts.

Emergency preparedness and continuity of business can be more important than some security measures. Relatively modest investments in emergency preparedness and continuity of business plans and capabilities may provide a much greater return on investment than large investments in security systems of dubious value. Risk-based assessments of maritime transportation facilities should address their emergency preparedness and continuity of business programs as well as their security programs, and prioritize enhancements in each area based on which will contribute the most to supporting overall US homeland security goals.

Recovery plans and capabilities. Recovery plans and capabilities are not new to the maritime transportation system; they have been in place for many years, particularly in areas of the nation routinely threatened by hurricanes. Additionally, Cold War defense planning included plans for restoring port operations and efforts to revive and adapt such planning to terrorist threats were begun after the 9/11 attacks in 2001. However, as the protracted recovery of Gulf Coast shipping after Hurricane Katrina shows, current plans and capabilities probably are not sufficient to prevent a large-scale terrorist attack on a critical node in the maritime transportation system from causing serious disruption of international trade and loss to the US economy. Three corrective actions are needed:

First, current planning is inadequate and too narrow in scope. The Maritime Incident Response Plan is woefully inadequate and does not address the full range of actions and capabilities that would be required to recover from a major terrorist incident. Plans and capabilities for rapid damage and channel blockage surveys, maritime infrastructure repair, and salvage and dredging to clear channels are inadequate.

Second, recovery plans must address the intermodal transportations system as an integrated whole, including road and rail transportation and pipelines as well as maritime transportation. Planning and recovery efforts for these various transportation modes currently proceeds independently, which could result in one mode being restored while another remains out of commission, thus preventing the restoration of cargo flows.

Third, investment in maritime transportation recovery capabilities is inadequate. The overwhelming focus of attention since the 9/11 attacks in 2001 has been on investment in security measures to prevent attacks. Investment in security needs to be balanced against investment in recovery capabilities. Many elements of the maritime transportation system are inherently vulnerable and no amount of spending on security measures will make them invulnerable to terrorist attack. On the other hand, taking a risk management approach and making prudent investment in recovery capabilities would greatly reduce the consequences of an attack.