



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Testimony of

Christopher Koch

President & CEO of the

World Shipping Council

Regarding

Maritime Transportation Security Act Oversight

Before the

**Senate Committee on
Commerce, Science, and Transportation**

May 17, 2005

Introduction

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify before you today. My name is Christopher Koch. I am President and CEO of the World Shipping Council, a non-profit trade association of over forty international ocean carriers, established to address public policy issues of interest and importance to the international liner shipping industry. The Council's members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry roughly 93% of the United States' imports and exports transported

by the international liner shipping industry, or more than \$500 billion worth of American foreign commerce per year.¹

I also serve as Chairman of the Department of Homeland Security's National Maritime Security Advisory Committee, as a member of the Departmental Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), and on the Department of Transportation's Marine Transportation System National Advisory Committee. It is a pleasure to be here today.

In 2004, American businesses imported 10 million loaded cargo containers into the United States. The liner shipping industry transports on average about \$1.5 billion worth of containerized goods through U.S. ports each day. In 2005, a projected 11% growth rates means that the industry will handle more than 11 million U.S. import container loads. In 2006, containerized trade growth is forecasted to increase another ten percent, and we will need to be ready to handle more than twelve million import containers. And these trade growth trends are not expected to stop after 2006.

Consider the requirements of one customer of our industry. Wal-Mart will import roughly 360,000 FEUs (forty foot containers) this year. If you were to place that volume on trucks bumper-to-bumper in a single line, it would stretch 3,750 miles. And those volumes have to be moved efficiently at the same time as L.L. Bean's, Target's, Home Depot's, Ford's, K Mart's, Procter & Gamble's, McDonald's, Hewlett Packard's, General Motors', General Electric's, Whirlpool's, Nike's, Becks Beer, Joe's Hardware Store, and thousands of other shippers.

The demands on all parties in the transportation sector to handle these large cargo volumes efficiently is both a major challenge and very important to the American economy.

At the same time that the industry is addressing the issues involved in efficiently moving over 11 million U.S. import containers this year, we also must continue to address the unfinished task of enhancing maritime security, and do so in a way that doesn't unreasonably hamper commerce.

The Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.

What is the appropriate collection of measures to address this challenge?

¹ A list of the Council's members can be found on the Council's website at www.worldshipping.org.

The Department of Homeland Security's maritime security efforts involve many different, but complementary, pieces, including implementing the directives of the Maritime Transportation Security Act (MTSA).

It includes the establishment of *vessel security* plans for all arriving vessels pursuant to the International Ship & Port Facility Security Code (ISPS Code) and Maritime Transportation Security Act (MTSA).

It includes the establishment of U.S. *port facility security* plans and area maritime security plans pursuant to the ISPS Code and MTSA, and the establishment by the Coast Guard of the International Port Security Program (IPSP) pursuant to which the Coast Guard visits foreign ports and terminals to share and align security practices and assess compliance with the ISPS Code.

The Coast Guard's efforts to implement these initiatives are well developed.

It includes the Maritime Domain Awareness program, under which DHS acquires enhanced information about vessel movements and deploys various technologies for better maritime surveillance. The challenge of effectively patrolling all the coasts and waters of the United States is obviously a large one.

The MTSA directives and DHS efforts also include enhanced security for *personnel* working in the maritime area, from the requirement that all foreign seafarers have individual visas if they are to get off a ship in the U.S., to the imminent promulgation of proposed rules on the Transportation Worker Identification Credential (TWIC). Regarding the TWIC, DHS officials have indicated their intent to issue a proposed rulemaking on this issue this summer. At the request of DHS, the National Maritime Security Advisory Committee, after intensive, open and constructive dialogue amongst diverse industry and government officials, approved last Friday a detailed set of recommendations to the Department for their consideration in the development of this ambitious initiative.

And last, but certainly not least, MTSA directives and DHS efforts include an array of initiatives to enhance *cargo security*, which the Committee staff has requested that I discuss. There are several elements and programs that comprise the government's cargo security strategy, and each has a role. This morning I'd like to briefly address the following cargo security issues:

- Cargo Security Risk Assessment Screening
- Radiation Inspection of all Containers
- Enhancing In-Transit Container Security
- The Container Security Initiative
- The C-TPAT Program
- The World Customs Organization
- Container Security Technology

1. Cargo Security Risk Assessment and the National Targeting Center

The stated and statutorily mandated strategy of the U.S. government is to conduct a security screening of containerized cargo shipments *before* they are loaded on a U.S. bound vessel in a foreign port. The World Shipping Council fully supports this strategy. The correct time and place for the cargo security screening is before the containers are loaded on a ship. Most cargo interests also appreciate the importance of this strategy, because they don't want their shipments aboard a vessel delayed because of a security concern that could arise regarding another cargo shipment aboard the ship.

In order to be able to perform this advance security screening, Customs and Border Protection (Customs or CBP) implemented the "24 Hour Rule" in early 2003, under which ocean carriers are required to provide Customs with their cargo manifest information regarding all containerized cargo shipments at least 24 hours before those containers are loaded onto the vessel in a foreign port. The Council supports this rule. Customs, at its National Targeting Center in Northern Virginia, then screens every shipment using its Automated Targeting System (ATS), which also uses various sources of intelligence information, to determine which containers should not be loaded aboard the vessel at the foreign port, which containers need to be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low-risk and able to be transported expeditiously and without further review. Every container shipment loaded on a vessel for the U.S. is screened through this system before vessel loading at the foreign load port.

The Department of Homeland Security's strategy is thus based on its performance of a security *screening* of relevant cargo shipment data for 100% of all containerized cargo shipments before vessel loading, and subsequent *inspections* of 100% of those containers that raise security issues after initial screening. Today, we understand that CBP inspects roughly 5.5-6% of all inbound containers (over 500,000 containers/year), using either X-ray or gamma ray technology (or both) or by physical devanning of the container.

We all have a strong interest in the government performing as effective a security screening as possible before vessel loading. Experience also shows that substantial disruptions to commerce can be avoided if security questions relating to a cargo shipment have been addressed prior to a vessel being loaded and sailing. Not only is credible advance cargo security screening necessary to the effort to try to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or incident recovery strategy.

Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to Customs for each shipment for the before-vessel-loading security screening is the ocean carrier's bill of lading/manifest data filed under the 24 Hour Rule. This was a good start, but carriers' manifest data has limitations.

Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities.² *Currently, there is no data that is required to be filed into ATS by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading security screening process, even though these parties possess shipment data that CBP officials believe would have security risk assessment relevance that is not available in the carriers' manifest filings, and notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted "prior to loading in a foreign port"*³. Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until after the cargo shipment is in the United States, often at its inland destination – too late to be used for security screening purposes.

Last fall, the COAC Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide Customs with the following data before vessel loading:

1. Better cargo description (carriers' manifest data is not always specific or precise)
2. Party that is selling the goods to the importer
3. Party that is purchasing the goods
4. Point of origin of the goods
5. Country from which the goods are exported
6. Ultimate consignee
7. Exporter representative
8. Name of broker (would seem relevant for security check.)
9. Origin of container shipment – the name and address of the business where the container was stuffed.

The Council agrees with this recommendation. The government's strategy today is to inspect containerized cargo on a risk-assessment basis. Accordingly, the government should improve the cargo shipment data it currently uses for its risk assessment. An ocean carrier's bill of lading by itself is not sufficient for cargo security screening. These cargo entry shipment data elements would improve cargo security screening capabilities. If a risk assessment strategy is to remain the core of the government's cargo security system, the government needs to decide what additional advance cargo shipment information it needs to do the job well, and it must require cargo interests, and not just carriers, to provide the relevant data in time to do the advance security screening. While this is not a simple task, a next step forward requiring shipper interests to provide more data on their cargo shipments before vessel loading is appropriate. CBP and DHS officials are currently reviewing this issue.

² See also, "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection", General Accounting Office Report and Testimony. March 31, 2004 (GAO-04-557T).

³ 46 U.S.C section 70116(b)(1). Section 343(a) of the Trade Act also requires that cargo information be provided by the party with the most direct knowledge of the information.

2. Radiation Screening

A particular security concern is the potential use of a container to transport a nuclear or radiological device. While there is no evidence that terrorists have nuclear weapons or devices, or that a shipping container would be a likely means to deliver such a device, the consequences of the potential threat – including those from a low tech “dirty bomb”-- are sufficiently great that, in addition to the targeted inspection of containers discussed above, CBP is deploying radiation scanning equipment at all major U.S container ports, with the objective of being able to check every container entering the U.S. for radiation by the end of this year. CBP and the Department of Energy are also working with foreign ports to encourage the installation of radiation scanning technology abroad as well.

We understand that the Government Accountability Office is currently reviewing the effectiveness of the radiation detection equipment being used, which is clearly an important issue.

3. Enhancing In-Transit Container Security

While the most important and challenging container security issue is ensuring that containers are loaded with cargo securely in the first place, it is also important to have a system that can help determine whether a container may have been tampered with while in-transit. In September 2003, the Council, together with National Industrial Transportation League and the Retail Industry Leaders Association, recommended to DHS that the government promulgate a container seal verification rule as the most practical way to address this issue in the near term. The Maritime Transportation Security Act Advisory Subcommittee of COAC made the same recommendation to DHS last fall. CBP and DHS are currently in the process of drafting proposed regulations on this issue. This will be a costly and challenging rule to implement, but we recognize the need to address this issue and the need for a container seal verification rulemaking.

Some of the more important issues that will need to be addressed in this rulemaking will be: the reporting process to CBP when a seal anomaly is identified, the consequences to the shipment when a seal anomaly is identified, where the seal verification is to take place, and a reasonable implementation time frame that will allow port facilities around the world to develop implementation measures.

4. Container Security Initiative

No nation by itself can protect international trade. International cooperation is essential. For ships and port facilities, the International Maritime Organization (IMO), a U.N. regulatory agency with international requirement setting authority, has responded to U.S. leadership and created the International Ship and Port Security Code (ISPS). These IMO rules are internationally applicable and are strictly enforced by the U.S. Coast Guard. There is no comparable international regulatory institution with rule writing

authority for international supply chain security. For a variety of reasons, the World Customs Organization (WCO) has not acquired such an authority.

At the WCO, CBP is working diligently with other governments on a supply chain security framework that can be used by all trading nations. This framework will be useful, but will remain at a fairly high level and will be implemented on a voluntary basis by interested governments. Consequently, U.S. and foreign customs authorities must also create a network of bilateral cooperative relationships to share information and to enhance trade security. This is the Container Security Initiative. The Council supports this program and the strategy behind it.

In March, Dubai became an operational CSI port, and Shanghai and Yantian are expected to become operational soon. When they are, more than 60% of U.S. containerized imports will be passing through operational CSI ports, with further program growth expected. The liner shipping industry is fully supportive of these efforts by Customs authorities and hopes the program will continue to expand as expeditiously as possible.⁴ A listing of operational, and soon to be operational, CSI ports follows:

Port Name	Total CY 2003 US Import TEUs (000)	Total CY 2004 US Imports TEUs (000)
Hong Kong	1,885.41	1,866.32
Yantian (Shenzhen)	1,603.83	1,982.79
Shanghai	937.34	1,278.50
Busan	891.38	971.49
Singapore	478.73	494.30
Rotterdam	420.90	427.75
Bremerhaven	415.99	392.18
Antwerp	262.21	304.60
Tokyo	250.77	267.53
Laem Chabang	186.68	201.06
Nagoya	169.04	174.94
Le Havre	154.93	139.67
Genoa	153.92	144.57
Le Spezia	143.69	159.67
Kobe	111.13	119.97
Hamburg	110.93	150.01
Algeciras	109.09	81.75
Gioia Tauro	103.96	104.48
Yokohama	82.781	109.02
Livorno (Leghorn)	80.15	92.33
Felixstowe	69.54	69.51
Tanjung Pelepas	64.71	45.96

⁴ On May 9, the Argentine government signed a declaration of principles to become involved in CSI. The expansion of CSI to Buenos Aires will be the first CSI cooperative agreement in Latin America.

Durban	41.57	43.94
Port Kelang	41.10	39.26
Naples	40.34	29.88
Southampton	40.28	38.62
Liverpool	38.85	39.37
Thamesport	31.49	32.34
Halifax	26.39	24.38
Gothenberg	17.46	18.81
Piraeus	10.92	11.58
Vancouver	5.74	13.59
Tilbury	5.23	2.56
Marseille	4.40	1.07
Dubai	1.20	1.11
Montreal	0.27	0.72
Zeebrugge	0.08	0.02

37 CSI Ports listed: 9,875.63 TEUs (thousands) to the U.S. in 2004
Total US Imports: 15,805.48 TEUs (thousands) in 2004
37 CSI Ports = 62.48% of total U.S. imports

One of the issues that the recent Government Accountability Office (GAO) report on CSI identified was that foreign Customs authorities are not inspecting at the foreign load port all of the containers that CBP has identified for security inspection. There are a number of relevant issues with respect to this finding, but I would note a couple of points.

First, understanding why these containers were not inspected at the foreign ports is very important. For example if it was because local Customs intelligence had good reasons to determine there was not a significant security risk, that fact would be obviously relevant.

Second, building cooperative Customs relationships requires time, commitment and mutual trust. In order for the CBP officials stationed in CSI ports to build trust and relationships with foreign customs authorities, the CBP program must be supported with professional personnel that have long-term assignments to these positions. Foreign customs authorities would have a difficult time building cooperative relationships if the CBP personnel must rotate out of their CSI positions after a short period of time. We understand that this has been an issue in the early phases of the CSI program, and hope that any difficulties CBP may have had in getting qualified, full time people stationed to these positions is being or has been resolved. CBP will need the full support of DHS and the Department of State to ensure an effective and robust CSI program.

Third, we note that the supply chain security framework that is being developed by the World Customs Organization (WCO) and is expected to be approved next month, provides an important reinforcing principle that should help the CSI program, namely that the Customs administrations of exporting nations should conduct outbound security inspection of high-risk containers at the reasonable request of the importing country.

This is an international affirmation of the CSI program's principles.

Finally, if CBP ever encounters a foreign customs authority that is unwilling to inspect a container that CBP believes is high risk, it can and should issue the ocean carrier a "Do Not Load" message and that container will not be loaded aboard a vessel destined for the U.S. There is no reason why any container that CBP has identified as "high risk" can't and shouldn't be stopped and inspected before it is loaded aboard a vessel bound for the U.S. If the container is not high risk but still one that CBP wishes to inspect, it can use its discretion to inspect it at the U.S. discharge port.

5. C-TPAT

C-TPAT is an initiative intended to increase supply chain security through voluntary, non-regulatory agreements with various industry sectors. Its primary focus is on the participation of U.S. importers, who are in turn urged to have their suppliers implement security measures all the way down their supply chains to the origin of the goods. This approach has an obvious attraction in the fact that the importer's suppliers in foreign countries are beyond the reach of U.S. regulatory jurisdiction. In return for participating in the program, importers are given a benefit of reduced cargo inspection. The C-TPAT program invites participation from other parties involved in the supply chain as well, including carriers, customs brokers, freight forwarders, U.S. port facilities, and a limited application to foreign manufacturers.

C-TPAT has improved the security of importers' supply chains. How much it has improved security is difficult to determine or measure. GAO has produced a critical study of C-TPAT, entitled "Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security". The program is currently under scrutiny by both Congress and DHS. It is facing both fair and unrealistic criticism.

C-TPAT needs to be understood for what it is and what it is not. C-TPAT is a set of voluntary, partnerships between CBP and willing industry members. C-TPAT is not a regulatory program. It should not be confused as being one. Nor should it be a substitute for regulations when the government has clear, specific things it wants industry to do to enhance security. The difficulty is that the program is in some respects ambiguous, and perhaps unavoidably so.

It is not a regulatory program, yet critics want specificity, strict enforcement, and penalties for non-compliance – features that characterize regulatory programs.

Its costs can be significant, but its benefits are necessarily limited; parties that are not importers receive no direct benefit from the program.

Its principal purpose is to try to affect the conduct of parties outside U.S. regulatory jurisdiction, yet some expect it to have an effect similar to what would occur if these parties were subject to U.S. regulatory jurisdiction.

It is a program that relies on participants' own risk assessment and allows participant's discretion and flexibility in application of the security standards. At the same time, the program tries to promote uniform and common standards of behavior through generalized "minimum standards".

When COAC posed questions that, in essence, asked what importers should do when some of their suppliers are compliant with C-TPAT standards and some are not, CBP responded in their Frequently Asked Questions that all of an importer's suppliers should be compliant or that the importer must demonstrate an ongoing commitment to get all suppliers compliant. Importers will face situations where they cannot require or ensure that all their suppliers are compliant. On the one hand, one can sympathize with the way the issue is being addressed, because CBP wants to keep pushing for full compliance, and because the program would become much more complicated if each importer's supply chain had to become divided into various levels of compliance or non-compliance. On the other hand, by not differentiating within importers' supply chains, one must either accept or not accept the proposition that each container shipment of a C-TPAT importer is likely to obtain an equivalent lowering of its risk assessment.

C-TPAT is a program that other nations' customs authorities and the WCO are examining and find conceptually attractive, yet its definition, its application and the extent of its utility are still in development and not yet settled here in the U.S. A common, global C-TPAT, "trusted shipper" type system might be a very good idea. At the same time, if many trading nations were to implement C-TPAT type programs in ways that significantly differ from each other, very significant complexities for international commerce could emerge, including the possibility of redundant and duplicative, or even inconsistent, efforts.

These are difficult issues, and one should temper criticism of the program with an appreciation for the fact that CBP has been trying very hard to make the program effectively address significant concerns in supply chain security in areas where it has no regulatory jurisdiction. The program is a voluntary, non-regulatory, evolving initiative.

Voluntary Partnerships: C-TPAT tries to provide general guidance for enhancing security with respect to some, but not all, aspects of supply chain security. It recognizes that flexibility in application is unavoidable when applied to the tens of thousands of different supply chains around the globe. For example, the new C-TPAT Importer Security Criteria have standards for fencing, facility lighting, and employee background checks and credential checking. C-TPAT importers can agree to communicate this to all their foreign suppliers and to urge their suppliers' compliance, but obviously not every business in the world involved in shipping goods to a U.S. C-TPAT importer is going to have compliant fencing, lighting, etc. This doesn't mean C-TPAT is a failure, or that a C-TPAT importer is a failure if one or more of its suppliers don't conform to the standard, and it doesn't mean that C-TPAT doesn't provide security enhancement. It means that there is an unavoidable degree of variability, imprecision and ambiguity in the program when it comes to its implementation.

Not a Regulatory Program: Many maritime and supply chains security issues can be, should be, and are addressed through regulatory requirements, not C-TPAT. For example, vessel security plans and port security plans are regulated by Coast Guard regulations implementing the ISPS Code and MTSA. The data that must be filed with CBP to facilitate cargo security screening must be addressed through uniformly applied regulations. Seafarer credentials and the Transportation Worker Identification Card must be addressed through uniformly applied requirements. Requirements to verify seals on import containers need to be addressed through regulations.

C-TPAT is a program that can try to address matters that are not or cannot be addressed by regulations, such as supply chain enhancements beyond U.S. regulatory jurisdiction, or matters that aren't covered by regulations, such as cooperating with CBP in providing access to information in support of investigative inquiries. C-TPAT may also be a platform from which CBP and program participants can analyze security vulnerabilities and problems and jointly develop plans that could more effectively try to address such situations. C-TPAT, however, should not be used in lieu of regulations when regulations are the more appropriate method to enhance security.

Validation: CBP has a C-TPAT validation program to confirm that participants are doing what they have said they would do, during which identified shortcomings can and should be discussed and remedial measures developed. However, the GAO report has criticized the program for conferring benefits to importers before validation has occurred and noted that the agency does not have adequate trained personnel to validate all C-TPAT participants in a timely manner.

This criticism is certainly welcomed by the private commercial security consulting business, which sees a substantial business opportunity if they can become government sanctioned security validators for C-TPAT type programs in the U.S. and around the world. Whether C-TPAT participants or the government would accept this role, how such a role would be defined and overseen, what the standards would be, whether validation by commercial parties would be required or voluntary -- are all issues that are undetermined at this time.

Compliance: C-TPAT is not a regulatory regime, with specific criteria that must be applied to everyone at all times. Some of the program criteria are very general, and its criteria do not cover all aspects of security. Further, a security failure in a specific case may not involve a lack of due care and may not involve a breach of the terms of the participant's C-TPAT Agreement.

Nevertheless, CBP has recently taken the position that it can suspend a C-TPAT participant from the program –

- a. Without advance notice, without discussion, and without an opportunity to cure the problem
- b. For matters that are not covered by the terms of the C-TPAT Agreement signed by CBP and the carrier (i.e., you can be kicked out of the C-TPAT program even if you have complied with the C-TPAT Agreement's terms)

- c. For any violation of law or significant security breach (e.g., drugs in a container, stowaways in a container)
- d. For an undefined duration.

Ocean carriers, which receive no direct benefits from CBP for participation in the program but have written their C-TPAT participation into many of their transportation contracts with shippers, have found this to be a surprising and troubling development at best. Carriers had believed that under a “voluntary partnership” program with CBP, specific security concerns would be jointly assessed to determine what measures could reasonably be taken to address any specific security shortcomings. To face no-notice suspension from a voluntary program that provides no direct benefits for events that may be highly unpredictable and under the control of third parties will significantly change the program and how it is perceived.

Evolving Initiative: C-TPAT is an evolving initiative, and industry and government will learn and adapt as it matures. For example, when the Sea Carrier portion of C-TPAT was formulated, there was no ISPS Code or Coast Guard MTSA regulation regarding vessel and port facility security plans, so C-TPAT carriers recognized the regulatory void and agreed to undertake a number of voluntary measures in this regard. Today, there are comprehensive Coast Guard regulations on these issues, and it is no longer appropriate for CBP to use C-TPAT to address the issues that the Coast Guard is addressing through its regulations. Similarly, carriers agreed in C-TPAT to participate in the electronic Automated Manifest System (AMS) for transmitting manifest information to CBP; at the time, paper manifest filings were possible. Now, electronic filing in AMS is required by regulation.

The future role of ocean carriers in C-TPAT will require further consideration and analysis. Carriers, unlike importer’s foreign suppliers, are regulated parties, and CBP and Coast Guard can and have established clear, uniformly applicable rules for them to follow. Furthermore, C-TPAT program benefits, which are basically less frequent cargo inspections, are importer benefits. Ocean carriers do not receive direct benefits from CBP for C-TPAT participation. How and where ocean carriers may fit in the program going forward remains to be seen.

As regulated entities, ocean carriers have a preference for clear, uniformly applied security regulations when an issue can be addressed through regulations. At the same time, we wish to continue to work with CBP and other DHS agencies to determine if there are appropriate ways to supplement the regulatory security regime. This will continue to require a partnership approach, clear communications, and mutual benefits.

Looking Ahead: C-TPAT is not the supply chain security strategy for the government – it is one layer and one piece of the evolving strategy. At the same time, the program’s critics have points that won’t be ignored. For example, it is difficult to believe that C-TPAT is presently sufficiently developed to actually be used as a determining criteria for what cargo would be allowed to be transported if the government had to respond to a terrorist incident involving a containerized cargo shipment, because,

among other things, there is uncertainty about whether all the suppliers in an importer's supply chain comply with adequate standards that warrant such confidence.

However, it is conceivable that the program may be able to attain this kind of result if the foreign suppliers that actually stuff the containers were included in the program. The fact that foreign manufacturers (except some Mexican manufacturers) and the parties stuffing the containers are not in the program means that the most important parties in container security aren't C-TPAT program participants. Could this be addressed by adding foreign manufacturers to the program?

Perhaps so, if C-TPAT were to be able to evolve from a program that gives benefits to U.S. importers if they undertake certain actions, to a program that would give those benefits to shipments where both the U.S. importer and a foreign manufacturer or container stuffer were certified as compliant with the appropriate standards. Is there a way for a program that is constrained by resources to achieve this additional extension? Perhaps yes.

CBP, under Commissioner Bonner's leadership, has been diligently developing international supply chain security standards at the World Customs Organization, and has undertaken discussions with the European Commission and various national governments. There is a possibility to develop these efforts into a more advanced, agreed internationalization of supply chain security improvements

6. The World Customs Organization

In some respects, the issues surrounding the C-TPAT program are similar to those that the World Customs Organization (WCO) has been grappling with since it established a special Task Force on Security and Trade Facilitation in 2002.

Currently, the WCO is finalizing a Framework of Standards to Secure and Facilitate Global Trade that is expected to be approved at the WCO Council next month. This initiative intends to establish international standards for Customs-to-Customs cooperation concerning cargo risk assessment, advance cargo information filing and common risk criteria, and for Customs-to-business partnership programs, like C-TPAT.

The establishment of international security standards and criteria for international supply chains and international cargo shipments is a sound and logical objective. The challenge, however, continues to be how to obtain implementation of such agreed-upon standards and criteria in the absence of a binding international instrument. The Framework and its supporting documents are expected to be approved by the WCO Council through a Recommendation that invites WCO members to implement it in accordance with individually established timeframes and each member country's capabilities. Thus, rather than early international acceptance and implementation of the Framework, we could see the Framework serve as an inducement for the establishment of bi- and multilateral Customs agreements where individual Customs authorities agree to

cooperate on the establishment of joint risk assessment programs, the advance filing of common cargo information and perhaps also on the mutual recognition of each other's partnership programs. To the extent such individual Customs agreements were to cover a "critical mass" of global trade, they could eventually establish the minimum standards that all trading nations would have to implement or risk seeing their export opportunities being curtailed.

Such a development would not happen over night. Nor would the attendant benefits for business in terms of mutual recognition and simplified and uniform filing requirements. But absent an international regulatory mechanism for supply chain and cargo security, it appears to be the only currently available option internationally for creating uniformity and commonality.

As noted earlier, however, it may also be a way for the C-TPAT type system to be extended to foreign manufacturers in those nations that make a serious commitment to establish and oversee C-TPAT type programs. Today, a U.S. importer is expected to "ensure" that a foreign supplier is following C-TPAT criteria – a pretty tough challenge. If reliable foreign authorities were to certify foreign manufacturers according to standards and procedures equivalent to CBP's certification of importers, confidence in enhanced security and shipper compliance could be greatly enhanced. This may not work in all nations, but it is certainly not inconceivable to see the U.S. accepting other responsible government program certifications of their manufacturers, and foreign governments' accepting U.S. certification of theirs. This model works for ships, where foreign government certifications are accepted (but also buttressed by strong U.S. port state enforcement), and it could be considered for supply chain security.

7. Technology and "Smart" Containers

Technology clearly has a role in increasing the efficiency and security of containerized cargo shipments. X-ray and gamma ray non-intrusive container inspection equipment is being deployed at U.S. and foreign ports, as are radiation portal monitors and radiation detectors.

In addition to these developments, there is a discussion of "smart" containers. What makes a container "smart", however, and what the appropriate technologies may be for such an objective remain unclear.

The Council and its Member lines have been working within the International Standards Organization RFID container technology working group on standards for electronic container seals, container tags and shipment tags. We expect that, once a seal verification requirement is imposed by U.S. regulation, these technologies will be seriously considered as an automated, efficient way to determine if containers have been tampered with while in transit.

There is also a discussion about the possibility of the application of shipper-applied “container security devices” (CSDs). The CSDs currently being tested by CBP only indicate whether one of the container doors has been opened. A properly applied e-seal may provide equivalent functionality. Explanations of what a CSD should accomplish vary, and a clear definition has not yet emerged. Furthermore, other issues about CSDs that have not been adequately addressed, including the radio frequency to be used and whether it would be compatible with the emerging ISO standard’s frequency for e-seals, who would read the devices, how would they know which boxes have CSDs to be read, where they would be read, who would be expected to build and operate the reading infrastructure, what would be done with the information, the devices’ reliability and accuracy, and what would be done with exception reporting.

There is also discussion of a “next generation” or “Advanced CSD” with more sophisticated sensors that DHS is researching, which will also need to address a number of issues, including what specifically is it that needs to be “sensed”, the accuracy and reliability of the device, its cost, who applies the device, the reading infrastructure that would be needed, who would read it when and where, and the protocols for how different readings would be addressed by whom and when.

The idea of transforming containers into “smart”, impregnable fortresses clearly has an appeal. Reality, however, requires addressing issues of: technology definition and standards; false positives from sensor technologies and their consequences; questions about device reliability; maintenance complexity; device failures and equipment out of service time; power needs and failures, including battery life issues; device costs; and labor issues and costs. In addition, technology can bring new security vulnerabilities that have to be considered. For example, permanent or reusable container security technology devices would require a capability to “write” new information into the device or amend existing information in the device. Such a capability would require a wide range of parties around the world to be given the capability of writing new information into container security devices, which would create troubling security vulnerabilities of third parties becoming capable of “hacking” into the devices. It is for this very reason that the ISO electronic seal standard will require that e-seals be one time use seals without the capability to write or change the information in the seal.

As different technology vendors jockey for position, some things are becoming clearer:

1. Industry and government need to cooperate and agree on what the security requirements are, and what the respective implementation roles of industry and government would be.
2. Cost does matter. A decision to invest in a particular technology applicable to the global container industry will be expensive and will require assurance that government is not likely to abruptly change requirements.

3. Whatever technology is chosen for application to international containerized cargo shipments, it will need to be a common, universally deployable technology.
4. Proprietary solutions that require a particular manufacturer's product or reading system will not be acceptable.
5. Technology vendors who push products that involve the vendor capturing, managing, and profiting from all the data generated from the device -- and there are a number of these -- are likely to encounter hard questions, if not strong resistance, from industry.

Cargo shipment data is the data of the carrier and the shipper, and with consent, their agents. It is appropriate for the importing and exporting nations' governments to have access to this data, but it is not appropriate for third parties to try to use technology to capture it and resell it to other commercial interests. Vendors who try to do this will need to address a number of policy and legal issues.

Summary

When addressing the issue of international supply chain security, we find ourselves dealing with the consequences of two of the more profound dynamics affecting the world today. One is the internationalization of the world economy, the remarkable growth of world trade, and the U.S. economy's appetite for imports – a demand that fills our ships, our ports, and our inland transportation infrastructure, a demand that will result in more than 11 million U.S. import containers this year, and more than 12 million next year, and a demand that will increasingly test our ability to move America's commerce as efficiently as we have in the past.

The other dynamic is the threat to our way of life from terrorists and the challenge of addressing the vulnerabilities that exist in the free flow of international trade, even when the specific risk is elusive or impossible to identify.

Finding the correct, reasonable balance between prudent security measures and overreacting in a way that impairs commerce is a tough challenge.

We are making real progress in addressing these challenges, but that the effort to address them more effectively must continue. In particular, it would be helpful to develop a blueprint or framework that identifies the specific security gaps and security requirements in the supply chain security system, so that government and industry can all understand, target and prioritize the development of appropriate solutions needed to address the appropriate, correct, and agreed requirements.

DHS continues to refine and extend its maritime and cargo security regime. This year we expect to see major rulemakings dealing with container seal verification requirements and with the issuance of Transportation Worker Identification Cards, a Departmental determination of what additional cargo shipment data needs to be given to CBP to enhance the cargos security screening system, and a continued review of the C-TPAT program.

Mr. Chairman, the World Shipping Council and our member companies believe that there is no task more important than helping the government develop effective maritime and cargo security initiatives that do not unduly impair the flow of commerce. We are pleased to offer the Committee our views and assistance in this effort.