

Introduction ... Who is NAWE?

Good afternoon, I'm Tay Yoshitani, the Senior Policy Advisor to the National Association of Waterfront Employers (NAWE), a national trade association which includes most of the large private sector marine terminal operators in the U.S. Briefly by way of background, prior to this role with NAWE, I served as Executive Director at both the Port of Oakland and Baltimore, and was the Deputy at the Port of Los Angeles (bio attached). On behalf of NAWE, I want to thank the members of the Senate Committee on Commerce, Science and Transportation for giving us the opportunity to comment on maritime cargo security and S. 1052.

NAWE members work closely with port authorities, ocean carriers, railroad and trucking companies, organized labor and shippers to ensure the smooth flow of international commerce that keeps our country's economy strong. It is estimated that the maritime industry handles about 15% of the U.S. GDP. Our membership reflects the international scope of the maritime industry and terminal operations. Many of the members are U.S. company-owned, but many are foreign-company owned as well. In fact, P&O Ports has long been an active member of NAWE and holds a seat on the Board of Directors.

NAWE has been involved with port security since concerns were first raised almost 10 years ago. This Association testified before this Committee on the initial Maritime Transportation Security Act (MTSA) several months before 9/11, and, since its passage, we have been involved with the Coast Guard, TSA, CBP, and other elements of DHS as MTSA-based security regulations, C-TPAT, and cargo inspection programs have been developed and implemented.

What Do Terminal Operators Do?

Recent events have brought much attention on the typical structure of most U.S. ports and what role terminal operators play. As you know, the vast majority of ports in the U.S. are publicly owned by a state or municipal authority. Typically, the port authority, as land and fixed

asset owner, leases out marine terminals to terminal operators but retains a multitude of important responsibilities. As terminal operators, our members typically lease property from ports and essentially conduct the business of loading and unloading cargo between ships and marine terminals. This sounds a bit simplistic, but it's not. On any given day, there may be several ships at berth with thousands of containers being loaded and unloaded, while a comparable number of trucks are entering and exiting our terminal to pick up or drop off a load. To do this day-in and day-out in a safe manner, while keeping track of where each container is and where it is supposed to go, is a daunting task.

It is worth noting that some terminal operators provide a service that is more limited in scope than what I have just described. For example, in some cases, private operators are pure stevedores, servicing terminals run by operating port authorities. Regardless of scope, we conduct our business in compliance with numerous federal statutes, regulations and policies. In this post 9/11 world, many of these are, of course, security related. In fact, we are perhaps one of the most federally regulated industries in the country.

What is a Terminal Operator's Role in Port and Cargo Chain Security?

Given recent interest in the role of marine terminal operators, I want to take a moment to clarify how we view our role, specifically with respect to port and cargo security. To do this, it's helpful to separate security issues into basically two categories. The first is "facility security" which includes the port in general and individual marine terminals. The MTSA clearly designates the Coast Guard as the lead authority on port facility security. Under Coast Guard regulations, terminal operators are required to submit a comprehensive Facility Security Plan (FSP) for approval. Subsequent to initial submission, the Coast Guard conducts regular audits as well as annual exercises. Terminal operators are well aware that failure to comply with this approved plan may be cause for closure of the facility. Needless to say, terminal operators take these plans, audits, and exercises very seriously.

In conjunction with the Coast Guard, the Port Authorities are also actively engaged in facility security matters. Many Port Authorities have their own Port Police Force while others have a contractual relationship with their respective municipal police authority. A typical lease between the port and terminal operator may include security requirements that are borne by the lessee. But ultimately, the terminal operator is responsible directly to the Coast Guard on terminal security matters.

One key aspect of facilities security is access control of people and equipment. NAWA is in strong support of the upcoming TWIC program. We have reached out on a number of occasions to both the Coast Guard and TSA regarding this program including a recent submission of a “white paper” (see Attachment A) that includes recommendations with respect to truck gates at marine terminals.

The second area of security is what we refer to as the “cargo chain.” Essentially, this refers to understanding “what is inside the container.” Much has been written about this aspect of security, and it is the area of risk that most concerns those who understand maritime industry. The terminal operator actually has very little to do with this aspect of security other than a supporting role of moving containers around under the direction of CBP/DHS. When CBP wishes to inspect a container, they notify the terminal operator of the box number only. They do not reveal the name of the shipper, content, origin, or destination.

The “business service” that terminal operators provide is measured in terms of the “container unit.” We need to know from the customer what the disposition of the container should be. Is it for pick-up by a local business by a trucking company? Is it to go to a nearby rail yard for transport to some inland destination? For our purposes, we don’t have a business interest in knowing the content of the container. We are not given this information and we do not track this information. The one exception is if there is hazardous cargo in a container. We would know this because it is included in the ocean carrier’s stowage plan, and these containers require special handling by the terminal operator. Of course, we are well aware that regulations are being drafted for “cargo chain security” as we speak. Although terminal operators will have

no responsibility for cargo within containers, these impending regulations may call for the terminal operator to play some role in making sure that container seals have not been breached. But here again, we anticipate that our role would be limited to reporting the breach to the proper authority and taking action only under that authority's direction.

We recognize that security is everyone's business and requires a public-private partnership. NAWE and all of its members have been working closely with our partners at the Coast Guard, Transportation Security Administration, and Customs and Border Protection. We were active members of the MTSA Subcommittee of the Commercial Operations Advisory Committee. We are currently involved in the ISO RFID electronic seals discussion that may ultimately establish the much needed standard for the industry. And, it is worthy to note that all of our members are C-TPAT compliant.

NAWE Perspective on Maritime Security Concept/Approach

NAWE is in full support and agreement with the approach that the public-private partnership is taking to address maritime facilities and cargo chain security.

1. The "layered approach" is rational and makes good sense. No system by itself will ever be perfect. It makes sense that the initial layers begin well before the container reaches our terminals. After screening and targeting, the 24-hour rule permits CBP to get manifest data before loading at the foreign port. CSI allows comprehensive vetting before vessel loading. And, finally, before reaching our terminals, the Coast Guard has the option to board a vessel before it enters our harbors. The layered approach minimizes the chance of a breach of the system.
2. "Risk mitigation" is also a critical element of the approach. This starts with risk assessment one container at a time. CBP must be able to narrow their focus and direct their attention to a manageable percentage of containers in order to physically inspect them.

3. "Pushing the borders out" is also an excellent approach for inbound cargo and goes hand-in-hand with the "layered approach." The CSI program and RPMs at foreign ports are examples of pushing the borders out. There are other developments such as the Integrated Container Inspection System (ICIS), though not yet fully tested, that hold promise of further strengthening this approach. The detection of problem containers needs to be well before they reach our terminals. The focus must be at the point of stuffing the container and loading on to a ship.
4. Controlling access to marine terminals using the impending TWIC program is also a good approach. However, at this point, it is our understanding that technology problems still exist with scanning of cards and biometric indicators. The accuracy rate of the TWIC system must be very high for the system to be effective. Subject to resolution of these problems, we are in strong support of this program and continue to urge early implementation.
5. We all recognize that this is an international business and security issues transcend international borders. Therefore, our solutions must be implemented with international cooperation. International standards must be agreed upon before various security programs can be implemented on a global basis.
6. And lastly, leveraging appropriate technology makes a lot of sense. Terminal operators are already employing various technologies such as OCR and RFID to not only improve operations but enhance security as well. We support the use of technologies as long as they are appropriate and fully tested.

We support all of these concepts/approaches. If all of these approaches could be fully implemented, overall security at the facilities and the cargo chain would be greatly enhanced.

Comments on S. 1052

We have reviewed the “Transportation Security Act” (S. 1052) using the six approaches and concepts that I just mentioned and find them to be consistent. Therefore, NAWA fully supports this Senate bill as currently written. In the interest of time, I wish to limit my comments to three key points. However, we would be happy to submit, in writing, responses to any questions you might have on any of the specific provisions of this bill.

1. Provisions indicate clear recognition that DHS must obtain more and better information about what is being loaded inside the container at the point of “stuffing.” This is followed by the upgrading of our Automated Targeting System. We believe this represents the most significant opportunity to improve cargo chain security. We are encouraged that this bill would do much to improve upon this critical area.
2. The CSI program is perhaps the most important effort to “push the borders out.” This bill includes provisions to continue and enhance this program. This program needs to be adequately funded and expanded as quickly as possible.
3. And, lastly, I’ll just mention that we are encouraged that leveraging technology is an important element of this bill. The number of containers entering and leaving the U.S. is expected to grow rapidly over the next couple of decades. There is no way that facility and cargo chain security can be significantly enhanced without advances in technology.

What Else Should DHS and Their Agencies Be Doing?

In conclusion, NAWA is in support of the overall approach that is being taken to improve maritime facilities and cargo chain security. We also support S. 1052. We understand and recognize that terminal operators do have an important role in this public-private partnership. We stand ready to do our part.

We are concerned about the pace at which progress is being made on the various fronts. Cargo chain security regulations and the TWIC program are two that come to mind. Both of these are complex, but they are vital to upgrading facility and cargo chain security. Proposed regulations should be issued as soon as possible. And we urge this Committee to continue to provide the resources and oversight to bring these programs to completion. Along with all our colleagues in this industry, members of NAWE have a direct and vested interest in overall maritime security. In this regard, NAWE has, in the past, offered to provide a “loaned executive” to both the Coast Guard and the TSA to provide industry expertise. We are respectful of the established rule making procedures but continue to stand by this offer.

My last note is to invite all members of this Senate Committee and members of your staff to visit one or more of our members’ terminals. I can promise you that it will be interesting and well worth the investment of your time. Please feel free to contact me or any of my colleagues at NAWE to coordinate a tour at a terminal that is convenient to you. I can assure you that our members would be delighted and honored to host a tour.

Again, thank you for the opportunity to address this Committee. I’d be happy to answer any questions you might have at the appropriate time.