FUTURE DEVELOPMENTS IN PORT SECURITY- A PORT POLICE PERSPECTIVE

I know I do not have to tell anyone here just how much the world changed after the terrorist attacks of September 11, 2001 in New York and Washington D.C.

In the U.S., we created a whole new arm of government, the Department of Homeland Security. We passed new laws and put strict new rules in place on air travel, and we made major changes in the way we operate our seaports. We were not alone in that effort. Everyone involved in international shipping realized new measures would be needed not only to protect our individual regions but also to keep world commerce moving.

Our government agencies took immediate and, in most cases, appropriate steps to respond to the terrorist attacks and the new era in world commerce that followed the attacks. I will discuss briefly what we have done to add protection in three key areas: facilities, vessels and port areas, and will provide my views on where we must go from here and how we should proceed.

The U.S. maritime transportation system is vital to our national and to the global economy. Over 95% of non-North American trade enters the country through U.S. seaports, and our seaports handle over $740 billion dollars and 2 billion tons of domestic and international freight annually. Our seaports and maritime transportation infrastructure face a myriad of threats from vessels, people and cargo, which move through them. Consistent with our approach to the overall War on Terrorism, our approach to seaport security calls for a layered defense that starts far beyond our mainland.

Immediately after the terrorist attacks some five years ago, the Port of Seattle and other ports on the West Coast of the United States increased their protective measures. Those moves, in cooperation with the United States Coast Guard and the United States Customs and Border Protection evolved into the national and international standards that became required of ports as of July 1, 2004.

Onshore facility security
The Port of Seattle owns and operates a number of facilities on Puget Sound, including recreational marinas, the Bell Harbor International Conference Center, site of the first APEC conference, our Port headquarters building, and facilities for the North Pacific fishing fleet. We also own cargo and cruise terminals that are operated by various tenants. In addition to our seaport operations we operate Sea-Tac International Airport. The Port contributes more than $34 billion annually to the economy of the State of Washington. In container business, combined with the Port of Tacoma, we are the third largest container "gateway" in North America. We are also one of the nation's fastest growing cruise ports, with this year seeing more than 700 thousand people sailing from Seattle.

As a first step, we took new initiatives to make sure our facilities, and those of our customers, were safe. These measures included lighting and security cameras, among other things, and were based on in-depth threat and vulnerability assessments. There are many probable avenues a threat or potential action could take against Port of Seattle facilities. Due to the public nature of the Port facilities they are open to attack from waterside, landside or from the air with either guided and controlled or unguided projectiles to include aircraft. There are no known specific terrorist threats against the Port of Seattle facilities at this time, but if history is a guide, we can anticipate that there could be disruptions from several fronts, which may impact the Port's ability to serve as a vital economic engine and provide a smooth venue for commerce.

All of our facilities have put new security plans in place, which comply with the requirements of the U.S. Coast Guard and the Maritime Transportation Security Act of 2002 (MTSA).

The U.S. federal government stepped forward with $500 million in grants for port security, including $10.5 million that came to the Port of Seattle, to help harden these facilities against possible future terrorist attack.

Some of these measures involved new technologies:
Vehicle and Cargo Inspection Systems (VACIS) use gamma ray technology to scan the contents of containers and compare the results to the cargo manifest.

Radiation Portal Monitors (RPM), which screen cars and trucks as well as cargo for radiation levels, are being put in place at all U.S. ports.

Security within the harbor
Ports also worked with federal agencies, terminal and vessel operators, shippers and others to integrate security measures. As of July 1, 2004, when the ISPS Code came into full effect, each ports cargo and cruise terminals and hazardous materials facilities were required to have in place a security plan that complies with the International Maritime Organization (IMO) standards, which require ship security plans for all vessels registered in United Nations member states.

Vessel security
All international cargo, chemical, oil and cruise ships; and ships and vessels carrying more than 150 passengers, are required to file security plans. Each ship to which the ISPS Code applies is subject to certain verifications of their security plan.

Offshore initiatives
We have also seen the start of some offshore initiatives to try to take this security perimeter out beyond our domestic ports.

One of the U.S. Customs and Border Protection (CBP) programs is the Container Security Initiative (CSI), which places CBP inspectors in large overseas ports enrolled in the program. Those inspectors' duties are to pre-screen cargo containers being shipped to the United States by identifying and inspecting high-risk containers before they are loaded on ships at their port of origin. This program is designed around four core elements: 1. Using automated information to identify and target high-risk containers 2. Pre-screening containers as high risk before they arrive at a U.S. port 3. Using detection technology to quickly pre-screen high-risk containers and 4. Using smart, tamper proof containers.

The Customs-Trade Partnership Against Terrorism program (C-TPAT) is one of the key international supply chain security initiatives implemented by CBP following 9-11. While applicable to all import transport modes, it has had a significant impact on ocean container import operations. The process relies heavily on the participant's internal oversight processes, with periodic validation by CBP.

U.S. Customs and Border Protection instituted the 24-Hour Rule requiring information on cargo destined for the United States is submitted through the CBP Automated Manifest System (AMS) by the carrier or by a "non-vessel operating common carrier" if they are AMS certified. This rule requires detailed descriptive information for all cargo. It requires cargo vessels entering U.S. ports to provide a cargo manifest 24 hours before leaving their last foreign port.

In addition, the U.S. Coast Guard requires notification by inbound cruise and cargo vessels of their last five ports-of-call and a crew list 96 hours before arriving in a U.S. port.

Another tool is the International Ship and Port Facility Security Code, (ISPS). The ISPS Code sets out to provide a secure environment for the transportation of cargo by sea. It also ensures that the organization transporting the cargo is able to demonstrate compliance at all times. One of our biggest weaknesses is the lack of reliable credentialing. This is the ability to provide a recognized proof of identity for each employee following background checks. All seafarers and transportation workers have ongoing contact with cargo. Examining every employee's history is a major requirement and undertaking. In the U.S., a new Transportation Worker Identification Card (TWIC) is currently being rolled out. This level of credentialing is a major step in securing the logistics and transportation infrastructure while giving employees the freedom of movement they need to do their jobs.

Finally, we have been working on various ways to ensure point-to-point verification of the global supply chain via experimental programs such as Operation Safe Commerce (OSC) and Safe and Secure Trade Lanes, (SST) both of which are efforts to find reliable and cost effective procedures and technologies to track containers from their point of origin to their final destination. The real time tracking of goods, together with the electronic transfer of information and documents will make the supply chain increasingly efficient, while reducing costs and providing tighter security.

The ports of Seattle and Tacoma, Los Angeles and Long Beach, as well as the Port of New York/New Jersey, the nation's top three container Load Centers are leading this program under direction of the OSC Oversight Committee.

Taken together, these efforts locally, nationally and internationally provide new levels of security.

However, we are clearly not doing enough to provide the level of security we need both to protect our ports and to ensure the continuity of global trade and a healthy global economy.

In the U.S., for example, we have 361 seaports and river ports which receive over 50,000 visits each year from more than 8,000 foreign-flagged vessels, carrying in excess of 10 million containers.

Imagine what would happen if a biological, chemical or other weapon of mass destruction were to arrive in one of our harbors. We are just one incident away from a real problem of massive proportions. Every U.S. port would shut down and global trade would stop. And we don't have the international system in place to get them up and operating again. Any such incident would have immediate effects on the world's economy as well as long-lasting effects on the port in which it occurred.

We in the United States have spent some $10 billion on airport security since 9-11 but only a fraction of that on the much more complicated problems confronting our seaports.

I can say without hesitation that in America, we have overreacted on airport security, and clearly have fallen short in protecting our seaports.

It is imperative for us in the maritime industry to develop international standards for supply chain security. We need to be sure that containers are documented, loaded securely and protected against tampering throughout their journey.

We need to put in place a set of internationally recognized standards to ensure the security of the world supply chain. We should work through international organizations such as the International Standards Organization, (ISO) the International Maritime Organization, (IMO) and the World Customs Organization (WCO) to make security standards as uniform and accepted as shipping charts or aircraft landing protocols are today.

These standards should be performance standards, not prescriptive standards. That means they should clearly define the hurdles that security measures need to clear, but they should not prescribe the method for doing so. We have to leave room for innovation in the technologies, tools and methods we employ.

What we need to do

In order to achieve the greatest return from our port security efforts we must rely on existing and emerging technology. Whatever processes we use to make our facilities more secure ought to also allow us to expedite the flow of goods through them. We must ensure that security begins before cargo ships enter our ports. We need to upgrade our Coast Guard ships and technology, and improve information and intelligence gathering and sharing. The continuation of many of the programs already in place and enhanced new programs is essential. One example is the recently introduced GreenLane Maritime Cargo Security Act. Co-sponsored by Senator Patty Murray of Washington State, this program has some excellent objectives. These include increasing security for cargo and seaports, minimizing closures of U.S. seaports in case of an accident or attack, providing layered security in the supply chain, “pushing out” U.S. borders, and focusing resources on suspect cargo.

Further expansion of Radiation detection monitors at all ports as well as the enhancement of Radio Frequency Identification systems technology will be critical to supply chain and facility security. We also must develop better tools for identifying high-risk cargo and passengers.

This will enable us both to increase security while at the same time we make the supply chain faster, more flexible, more reliable and certainly more secure.

It is our duty to ensure the safety of our individual regions and the continuation of world commerce. I want to thank the Association and sponsors of this conference for providing the leadership in brining these issues before such a distinguished gathering. It is only through such shared knowledge and the exchange of ideas and concepts that we can add quality to our businesses and lives while we defeat those that would use terrorism to physically harm us and disrupt our economies.

Thank you.
Tim Kimsey