

Vikram Verma
President and CEO
Savi Technology

Presentation to the Subcommittee on Surface Transportation and Merchant Marine of US Senate Committee on Commerce, Science, and Transportation

Senator Wyden, Members, and Distinguished Guests,

I want to thank you for giving me the opportunity to provide testimony to the Committee on what I believe is one of the most important national security issues facing the United States.

To begin, I have three comments on the nature of the threats we are facing.

First, the container security threat is real. Although it is virtually impossible to predict the precise target or method that terrorists may deploy in their war on the civilized world, we can with confidence predict that, in all likelihood, the U.S. and other developed nations will continue to be the target of further terrorist activities.

With the expectation that that we will be attacked, we must look at the world through the eyes of a terrorist in order to determine what is likely to be the next target. What is both accessible and can be destroyed or leveraged to create maximum societal and economic disruption and damage? The global supply chain is one such target and it is especially vulnerable to terrorist attack.

The characteristics of an efficient, lean, high-velocity global supply chain – openness, ubiquity, diversity, agility - are also why it is an extremely attractive target for terrorists. The global supply chain is an accessible and tremendously efficient delivery system whose reach can allow a terrorist to strike virtually anywhere in the world – with potentially catastrophic results.

In addition – the supply chain is the foundation of the economy. The health and well being of our economy is directly tied to the continuous availability of efficient freight transportation. It has been estimated that a disruption that shuts down the global supply chain will cost the world economy \$1 Trillion dollars per week. Sinister elements wanting to destabilize the economies of the US and other industrial nations are certainly aware of this direct linkage.

Secondly, the threat is systemic. The vulnerability of the supply chain must be viewed from two perspectives; point attacks against a single element and systemic attacks against the infrastructure as a whole. Because of the decentralized and redundant character of the freight system, many believed that systemic vulnerability was low. September 11 showed that terrorists could carry out operations that are

more complex. This made us more aware of systemic risks via indirect attack upon the overarching interconnected, interdependent transportation infrastructure.

With over 300,000 miles of freight rail networks, 45,000 miles of interstate freeway, 600,000 bridges, 500 commercial airports, and several hundred of ocean freight terminals handling 16 million containers every year – the physical infrastructure supporting freight transportation is vast and poses a tremendous challenge to effectively monitor, safeguard and control.

Solutions designed to prevent point attacks will not work for the supply chain. Though extremely complex, we must look at the problem holistically – and put in place a security system that is capable of being as ubiquitous and flexible as the supply chain itself. This system must leverage best-of-breed technologies and proven processes to integrate the various components of the transportation system into a single command and control infrastructure that deters and prevents terrorists from using the supply chain for their activities, and also provides authorities the means by which to continuously monitor the supply chain and intelligently respond to security threats as they occur.

Thirdly, the threat is asymmetric. As has been widely discussed, full frontal conflicts – much like the Gulf War – are probably a thing of the past. Terrorist organizations will leverage their strengths of radically decentralized organizations with fervent followers employing low tech means to attack the U.S. We cannot respond on the same terms.

Now, what is to be our response to the ongoing asymmetric, systemic, real threats in port and maritime security?

First, as many of you have said, there is no single solution. We need effective intelligence, deterrence, monitoring and tracking, and response capabilities to secure the global supply chain. These capabilities however must be delivered through an integrated, comprehensive, systems-based approach that spans policy, security procedures, business practices and technology. With respect to technology, given the asymmetrical nature of the conflict, we need to employ high-tech means to prevent low-tech attacks. Equally as important, all participants in the global supply chain from port operators to port workers to global importers and exporters to shipping lines to technology companies need to work together.

Secondly, in terms of the policy response, we believe Congress is moving in the right direction. The Committee's legislation on maritime security is thoughtful and measured. We especially view the considered policy of a "cargo grading system based on secure supply chain systems" to be an important policy since it will not only enable secure *and fast* tradelanes, it also enables a system with a 'reset' button (so to speak) should any terrorist incident occur. This is a vital point: if we shut down the nation's ports indefinitely or even for several days in the event of an

incident, we will hand the terrorists a multi-trillion dollar win. We simply must keep the supply chain running securely and smoothly.

The Senate Subcommittee's legislation on the implementing of an "Operation Safe Commerce" program is also very positive in my view. The concepts of Operation Safe Commerce get to the physical nature of a complex problem, specifically:

- The development of auditable security standards for maintaining secure loading docks and ports
- The outfitting of containers with mechanical and/or electronic seals and devices intended to identify containers whose security has been compromised
- The establishment of integrated communication systems to track containers throughout the the entirety of their journey through the global supply chain
- The transmission of that tracking data in accessible format to appropriate Federal agencies
- The demonstration of secure trading lanes that ensure maritime and container security from point of origin to point of destination
- The establishment of new requirements which will pertain to all participants in the supply chain to allow Federal agencies sufficient information on the contents of each container and its expected journey.

All of these are vital requirements that not only add security to the system but will also result in efficiency benefits with better tracking, monitoring, and visibility capabilities. Further, ports and global importers and exporters are the key strategic control points in implementing these standards.

Finally, US Agencies are also taking positive proactive measures to secure the nation's transportation network and supply chain. Admiral Loy and the Coast Guard were especially admirable the day of and immediately after 9/11. They have taken that momentum and have instituted new security policies and procedures as well as have recruited a volunteer network to help monitor our nation's ports.

US Customs and Commissioner Bonner have been actively pursuing raising the security of the global supply chain through:

1. The Customs Trade Partnership Against Terrorism (CTPAT) Program
2. Customs' Container Security Initiative (CSI)
3. Bilateral agreements with our top trading partners

A third point, I would like to strongly emphasize is that this is no time for science experiments in process or technology. In a conversation I had both in April and just last week with the CEO of one of the largest port operators in the world, he is convinced there will be an incident in the global supply chain. We must use proven, reliable immediately available technology to address these threats now. We must leverage existing best practices currently in use.

Pilots and “proof of concept” projects are being proposed that will take years to complete. Then – and only then – can you begin the time consuming task of actually implementing the tools, technologies, and processes that will address the problem.

Fortunately – there are technologies and best practices available today that are proven, reliable, and can immediately be put to use to ensure the safety and security of our supply chain. One model I want to share with you is the Department of Defense’s Total Asset Visibility Network.

After the Gulf War, the U.S. Department of Defense began testing and implementing innovative track and trace technologies to gain comprehensive visibility of the supply chain as well as acquire “in the box” visibility. This led to the development of the world’s largest active radio frequency identification (RFID) network, spanning 36 countries, 350 nodes at seaports, airports, rail terminals, and military bases, tracking 250,000 conveyances as they move around the world. The DOD has named this global logistics infrastructure the Total Asset Visibility network.

The Total Asset Visibility network is comprised of active RFID tags that support full electronic container manifests and the ability to seal and secure intermodal containers from the loading point at manufacture through truck, train and ship transport. Once these seal tags are affixed to containers – essentially making these containers “smart” - wireless readers deployed at strategic checkpoints worldwide, most prominently in ports, feeds real-time information on the status, location, and other events into a global asset management software application. The Total Asset Visibility Network enables the DoD to track, locate, and secure all enroute containers.

Over the last seven years the system has been battle tested across over 5 continents, runs at 99.999% uptime, and has been used to track all military deployments from weapons to boots to foodstuffs. While the system was designed and the infrastructure was deployed to track all Department of Defense supplies leaving the country and landing in foreign ports, it can be used just as efficiently to track all goods entering the country with active RFID seal tags being applied at foreign port of origin by certified parties.

Total Asset Visibility could enable U.S. authorities – US Customs, the U.S. Department of Transportation (DOT) Transportation Security Agency (TSA), and the Office of Homeland Security -- to physically track and trace containers’ physical movements from the manufacturer’s dock to the U.S. port of discharge and beyond. Electronic active RFID seal tags on containers enable a security layer to detect potential intrusions and tampers. Alerts and exceptions can be programmed into the Total Asset Visibility network to automatically alert authorities of suspect container movements and to locate questionable containers quickly. Further, hazardous materials shipment information can be encrypted and tracked on electronic manifests affixed to containers to increase security and safety.

Why do I know so much about this system and its benefits? Because my company, Savi Technology, developed and implemented the TAV network for the Department of Defense and we are continuing to operate and extend the system for commercial applications. Based on agreement with the Dept. of Defense, this global infrastructure can readily be made available for commercial security use. In short, the US DOD, one of the largest shippers in the world, has invested over \$200M of the public's money to build a visible and secure global shipping network for their supply chain. To the extent that best practices and available technologies are considered, we feel this provides a rapid capability to address the principles of Operation Safe Commerce and Customs Container Security Initiative.

In summation, the supply chain is vulnerable; the threats are real and immediate. The problem is complex – and no simple, point solution will be adequate to address the problem. There are systems already in place based on proven, reliable technologies and processes that can be immediately leveraged to create a comprehensive system that will deter and prevent security breaches and will enable authorities to efficiently monitor and immediately respond to events that occur in the supply chain. I urge the members of this subcommittee to move quickly and expediently to make these systems available for the sake of the continued safety and security of our economy, our country, and most importantly our people.

Once again, I appreciate the opportunity to address the Committee and further welcome any questions.