I’d like to expand on the discussion of freight security and focus on two issues that have been raised by previous speakers: the need to

• assess vulnerabilities, as well as
• assess economic impacts.

At Argonne, we do a lot with vulnerability assessment. Historically, Argonne’s roots go back to the development of the world’s first nuclear fission reactor in the 40’s. Over the decades, we developed most of the major reactor innovations, and we also developed strong safety and risk assessment tools along the way. As a result, today we’re doing a lot of critical infrastructure vulnerability assessment, including for the transportation infrastructure.

Our cargo/freight system is very large and complex. It developed gradually overtime to become a complex, loosely integrated weave of commercial and non-commercial organizations. While regulated, it is also an open system.

There are positive aspects to this. When the Twin Towers of the World Trade Center were hit, air cargo came to a screeching halt, but surface freight continued unabated. However, due to its vast scale, complexity, and openness, we have no way of knowing for the most part what it is that is moving through the system at any given time. 890 million tons of goods and 7.8 million containers come into the country each year. Only a fraction of cargo that comes in to the country is inspected (in the neighborhood of 2-4%). Plus, there is

• 6000 miles of borders with Canada and Mexico
• >100 seaports in the U.S.
• 4M miles of highways in the U.S.

Like I said, the system and associated problems are big and complex.

In recent years, in America’s unceasing attempts to improve productivity, we have actually introduced risk into the system by taking out the waste (and thus the redundancy).

We have vulnerabilities due to our dependence on foreign oil to fuel the conveyance of goods. Any disruption of oil would cause us much pain.

We also have limited highway capacity which causes choke points in surface freight, as we see along the Gary-Chicago-Milwaukee corridor. Oh, and did I mention that freight is projected to double by 2020 – as it doubled in the previous 20 yrs.
Critical infrastructure like bridges and tunnels are costly and take years to replace, so we’re vulnerable in many ways.

Risk assessments are vital to help us to see where we must focus resources to get the biggest benefit, and also help suggest ways to direct policy as well as investment to good cause.

I also want to point out that this is very much a local issue.

- The Midwest region centered at Chicago is the largest freight center in the U.S. -- not NY or LA.
- We’re the 3rd busiest container handler in the world (behind Hong Kong and Singapore).

Other presenters also touched on economic impacts of security.

Freight is also vital to our economy. It gives us 10% of our economy. When you add international freight, freight touches 25% of our economy.

Improved productivity of freight transportation and logistics has been an engine of prosperity and competitive advantage, reducing total costs of production and freeing resources for other uses. Business logistics costs dropped from 16.1 percent of U.S. GDP in 1980 to 10.1 percent in 2000. Businesses made such progress by taking advantage of deregulation and applying information technology. They knit business functions together, collaborated across company boundaries, and increased efficiency through the disciplines of supply chain management. As inventories dropped, so did inventory variability and the variability of demand on transportation. The six percent reduction in GDP share over twenty years generated a benefit, in 2000 alone, of up to $600 billion in a $10 trillion economy.

We recently held a security workshop at Argonne, and someone made the analogy that our area highways were the conveyor belts for just in time delivery of inventory. It is a great mental picture of how our highways and surface freight industry have supported the important productivity improvements in the U.S. that fueled our economy.

Freight transportation and the logistics systems have become lean and tightly coupled, but progress also created new risks. I mentioned that these improvements have added risk by reducing redundancy in the system. Predictability and reliable deliveries are critical for freight, and these can be negatively impacted by measures designed to improve security.

Our laboratory has frequent dealings with TSA on technology to improve border and transportation security, and they are keenly aware that we must improve security, but not at the expense of commerce. This is keenly aware that we must improve security, but not at the expense of commerce. This is like throwing the baby out with the bath water. We must carefully balance risks. When you think about it, terror does not easily lend itself to measured response. By its very nature, it produces an enormous reflex. The terrorists brought down three planes, so the public stopped flying, thereby actually increasing their
risk by driving more. In an article entitled “Flying and Driving after the September 11 Attack” in American Scientist, the author calculates driving is roughly 100 times riskier than flying. Remember, we have over 40,000 driving fatalities per year in the U.S.

When I was younger and had just gotten married, I began taking flying lessons. My wife was OK with it, but my mother-in-law cut out every newspaper article on air crashes she could find for me. I would point out, “this one is in Peru, and this one is in Siberia. They don’t even cover auto deaths in the Chicago papers because it would take up too much space.” I finally said if I do die while taking up flying, it will probably be while driving to the airport. She stopped and thought for a moment, and then said, that’s another reason to stop taking lessons. I couldn’t win….

One last point I’d like to make is the role of technology.

Most of us here are involved with technology in one way or another. It is not a hard sell. The fact is, the volumes are so high in freight that you have to use technology to improve security. You can’t do it with people and process. There’s too much cargo coming in and moving through the system.

I’m sure you’re aware of the Container Security Initiative, which has four core elements:

- **First, identify "high-risk" containers.** These include any containers that may contain - based on intelligence and risk targeting principles - terrorist weapons, or even terrorists.

- **Second, pre-screen containers before they are shipped.**

- **Third, use technology to pre-screen the high-risk containers**, so that it can be done rapidly without materially slowing down the movement of trade.

- **Fourth, use smarter, more secure containers** - containers where customs officials will be able to tell if a container has been tampered with.

At our workshop at Argonne, we had some folks from the freight trucking industry. They operate on slim margins, and are very concerned about the cost of security. They want government to pay for it, but it costs a lot. Government thinks security is good business, and wants the commercial sector to carry its share of the burden. Remember how the Tylenol® tampering episodes caused the industry to adopt secure, tamper-proof packaging. So, sometimes it can become good business practice…

So what do freight companies think about adopting security technology? A criterion for security technology acceptance that we heard from one company was:

- Dual Use (improved security against terror causes substantial drop in fraud, drug trafficking)

- National standards, so it doesn’t become obsolete after they make substantial investment (although sometimes you can’t wait)
• Integrated, needs to work with existing infrastructures and processes (in other words, painless to use)
• Reliable and cheap! It has to actually work when you need it.

That’s a real challenge in some cases, because we may need zillions of sensors. Ultra reliability is probably too costly, so we really need redundancy to achieve dependability.

I read an interesting book a couple years back, called *EMERGENCE – the connected lives of ants, brains, cities, and software*, by Steven Johnson. It looks at a number of interesting simple biological systems, including slime molds and ant colonies, which exhibit emergent complexity and intelligence, even though composed of numerous simple behavior units. Many scientists are studying emergent behavior in nature to figure out how to make smart reliable systems to solve complex problems from cheap simple components. I think systems of sensors applied to security problems are one possible application. For example, if we could use a distributed system of simple sensors that act in a coordinate fashion, we have a hope of eventually catching something bad by taking different looks as it works its way through our freight system.

Thank you very much.