Smart containers—containers that use sensors and systems to track and report on much more than physical location—hold huge promise for improving supply chain efficiencies. And for strengthening U.S. national security, indeed security worldwide. But if smart containers are to realize their powerful potential, new technology challenges must be met and new incentives must be forthcoming from the federal government.

In November, my company received a phone call from a law firm asking about my availability as an expert witness. The case involved cargo security—a loss of both trailer and contents. The issue was quite simple. If container security systems were available at the time of the loss, and none was used, was there a liability issue? In other words, does the concept of “a reasonable standard of care” mean that negligence could be proven if container systems were reasonably available but not employed, especially for high-valued shipments? In the private sector, a negligence judgment could send shivers up the spines of carriers and shippers alike. It could imperil the promise of greater supply chain efficiencies.

These days, there are more and more of what are called “smart containers”—the electronic tracking and reporting systems and infrastructure, and of course the boxes themselves. The Homeland Security Research Group has estimated that revenues in the overall container security market will increase from less than $1 billion in 2007 to more than $4 billion in 2012. (See Exhibit 1.)

Most supply chain executives understand that smart containers can detect something, but little more is known or appreciated. In fact, not all smart containers have the same levels of intelligence. Basically, a smart box senses and reports. The smartest type tells who supervised its stuffing: what’s in it, where it’s leaving from and where it’s going, who’s carrying it, where it is at any given time, where it is but shouldn’t be, and whether an authorized person opens it at destination. It will also signal any unauthorized access en-route and say where that access took place. The dumbest container usually can tell you if its doors were opened en route.

So far, there are varying claims of benefits to the private sector for using smart containers and their associ-
CONTAINERS

ated technologies and systems. A recent study from Stanford University points to quantifiable benefits such as a 50 percent increase in access to supply chain data, a 38 percent drop in theft and similar losses, a 14 percent cut in excess inventory, and 29 percent reductions in overall transit times. Consulting firm BearingPoint has calculated benefits of up to $700 per container per move while the U.S. Congressional Budget Office has noted savings of 0.8 percent of the value of a smart container’s contents.

But the business benefits are only part of what smart containers can do. They also offer enormous potential to improve national security worldwide. Although sensing and reporting technologies can do a fine job of tracking a container’s physical location and whether it has been broken into or not, they cannot reliably determine
whether, for example, the cargo includes enriched uranium or biochemical weapons.

The challenge for supply chain managers is to divide the two objectives—supply chain efficiency and national security—and to set expectations accordingly. In this article, I certainly want to add to the understanding of what a smart container is by explaining what it detects, how it detects, what it does with what it detects, and how it “knows” when to begin and end working. But I also want to demonstrate why the U.S. government must provide more tangible incentives if the private sector is to be expected to fund smart container investments that will yield more than greater supply chain visibility and faster shipment transit times.

Let us start with some of the basics:

**What Should Be Detected?**
The easy response is that it depends! If you are Coca-Cola and you’re shipping syrup from Puerto Rico to the U.S. mainland, you probably aren’t worried about theft since thieves are unlikely to be able to move stolen syrup and because it’s probably not worth stealing in the first place. A more practical worry is contamination of the syrup—deliberate or otherwise. If you work for a pharmaceutical company like Pfizer, you’ll also fear contamination, but you’ll also worry about theft of high-value medications.

But the bigger question is about what is valued more: the product or the company’s reputation. Containers can (and often do) carry more than legitimate cargo. In the U.S., government mandates such as the SAFE Port Act require the detection of radiological materials. (This is echoed in the Implementing Regulations of the 9/11 Commission Act of 2007, which also mandates cargo security for all modes of transportation. We also have the Air Cargo Security Act of 2003.) Coca-Cola may also be worried about the consequences of one of its containers being a host for a nuclear device destined for detonation when it arrives in the United States. And what if your company ships highly radioactive materials? The primary concern will almost certainly be about terrorism.

There’s a difference between what should be detected in the private sector and what makes sense in the public sector. Government needs are likely to be more comprehensive. In addition to theft concerns, detection will include the need to detect weapons of mass destruction, including chemical, biological, and nuclear materials. The smart container must also detect illegal drugs and human cargo.

Not long ago, a major U.S. motor carrier opened a container of products originating in Mexico. Inside, the trucking company found evidence of non-paying passengers: cans of tuna, both opened and unopened, items of clothing and plastic bags containing urine. Plus, there was a hole in the roof that was never discovered in transit to the United States.

Although the specifics of what to detect vary by the type of shipper, there is some general agreement. The first order of business is to detect any unauthorized breach through any part of a container—not just through the doors. Second: it’s necessary to detect the container’s internal environment for the safety of the product being carried. And third, one must detect the presence of cargo such as weapons, illegal drugs, and human beings.

Those primary detection requirements can be supplemented by detecting the container’s location. If you work for Home Depot, for instance, you’ll want to know exactly where incoming containers are—especially if they are carrying products in high demand for a recent promotion. One location-detection option is called geofencing. In essence, the container detects a variance between where it should be and where it is—as a result of a hijacking, for instance, or if it has simply been sent to the wrong consignee or the wrong location.

What we should be able to detect, however, may not be what we can detect, given the current levels of technological sophistication.

**How Is Detection Accomplished?**
Sensors that can detect and report a breach or change in container status in real time or almost real time virtually extend the U.S. borders to foreign locations. It would be easy to think that today’s technology is more than sophisticated enough to handle the detection situations described, but that’s not so. Here’s what is possible now.

In most cases, basic detection is available and inexpensive. We can detect breaches into containers using magnetic switches, light, vibration, temperature, and more. Companies such as General Electric and GlobalTrak offer systems that use a combination of sensors, RFID (radio frequency identification), and satellite technologies to detect unauthorized breaches. Detecting a container’s position is also quite simple and low-cost.
Just as General Motors’ OnStar system uses satellite positioning to pinpoint location, so carriers and shippers can use services provided by satellite service providers such as Iridium, Orbcomm, and Inmarsat.

However, we still lack the sensing technologies needed to adequately detect biological agents, chemical agents, shielded enriched uranium, humans, explosives, and drugs—the issues that governments are likely to consider the most important. The technologies are still in the early stages of development. Moreover, when appropriate sensors do become available, the cost will be high.

That said, some advanced sensors are already available for use with containers. For instance, although we do not yet have the technology required for non-intrusive portal machines that can scan containers for an instant read-out on the presence of shielded enriched uranium, it is currently possible to detect the presence of shielded uranium over time. This technology takes advantage of long container voyages and close proximity to potential sources of uranium to sense radiation. At the same time, emerging applications of electrochemical and electromagnetic technology suggest the continued development and production of sophisticated sensors that will be able to detect the presence of WMD, drugs, and humans in containers and trailers.

What Is Done With What Is Detected?
There is a risk of focusing too much on detection and not enough on its usage. A smart container must be capable of reporting what it detects. There are currently three generally accepted methods of transmitting such data: RFID, satellite, and cellular. Users almost always trumpet the benefits of the application they employ. But it’s important to take a closer look at pros and cons of each.

RFID—Plenty of Challenges
RFID technology in logistics is not new, of course. Wal-Mart and Target are two of its best-known proponents. But the problems of RFID are many. Although the larger companies in the smart container sector indicate that they are committed to RFID, we believe their commitment will be short-lived.

One of the most serious problems can be seen by revisiting RFID’s operating principles. RFID applications require the carriage and transmission of data through a wireless system. Changes in the status of an RFID-tagged container can be sensed and transmitted when the container is interrogated by a transceiver positioned along the global supply chain. The transceiver sends out the triggering frequency, which produces a return transmission of any change in the container’s status—for example, if the doors have been opened. Since the data travels via electromagnetic waves, successful transmission depends on the use of the proper frequencies and the absence of noise or same-frequency emissions from competing antennas whose direction unintentionally or intentionally obstructs the intended RFID transmissions of the intended transponder.

In practice, a truly effective security solution requires a complete system of end-to-end coverage—from a container’s origin to its destination.

In fact, the approved use of RFID at U.S. seaports is a major security vulnerability. A perfectly benign RFID signal can be used to detonate an explosive device when the container is interrogated. On Nov. 13, 2007, that was demonstrated all too plainly by a group comprising Raytheon, Zapata Engineering, the University of North Carolina, Charlotte, my company, the local police squad, and 321 Equipment, a container supplier. A container carrying an explosive device was detonated by using the exact RFID signal approved and mandated for use in U.S. seaports. Officials from the U.S. Department of Defense were on hand to witness and validate the demonstration.

Additionally, RFID has no global protocols or standards. For instance, RFID on which the data ride in the U.S. will not work anywhere else. A transceiver in Shanghai or Cape Town cannot trigger data transmission on the tag on a container shipped from Boston or Jacksonville. In short, RFID for container security is applicable only to those areas of the world that have agreed on the same frequency.

An equally troublesome concern is the overland movement of containers and the corresponding creation of a land-based infrastructure of antennas and readers. Unlike RFID tags used in products and pallets that are read in controlled distribution systems, active RFID devices in containers that move through uncontrolled environments worldwide require the construction of antennas at chokepoints—the points of the container’s journey that cannot be circumvented by the carrier.

Satellite Communications—Stuck in Orbit
In general, there are two broad categories of satellite
Smart Containers

systems, both used for tracking and identifying containers and trailers. The most widely known are geostationary—satellites traveling approximately 36,000 kilometers high around the equator and rotating with the Earth so that they appear to be stationary. Inmarsat is one example, offering voice, broadband and satellite phone service. The second category is low-Earth-orbit (LEO) satellites, which orbit about 800 kilometers up and do not rotate with the Earth. LEO constellation owners such as Iridium or Orbcomm provide 24-hour communication service at multiple gateway control centers that receive, manage and forward communications from their satellites to locations worldwide. Combined with such round-the-clock communications, satellite systems can get around the challenges posed by land-based infrastructure of RFID antennas and readers.

The U.S. government must provide more tangible incentives if the private sector is to be expected to fund smart container investments that will yield more than just supply chain visibility and faster shipment transit times.

However, it is important to note the distinction between satellite tracking and satellite communications. Tracking, where a satellite “pings” a container that has a GPS (global positioning system) antenna, may be fine for asset management but inadequate for container security and control. For a container to declare its location to those who want to know, it must have another antenna to send the signal. Sophisticated two-way satellite communications require this additional antenna and a modem along with circuitry that allows the container to talk to its satellite provider under certain conditions.

GPS systems are not without weaknesses; they often have dead spots and they require visible antennas on the conveyance. A visible antenna might seem harmless, but it allows those who intend to hijack or breach a container to do so without detection. Secondly, the capacity to sense what is going on inside the container and to report back requires greater electronic sophistication than that needed for tracking alone.

Cellular Communications—Up in the Air

Cellular communication is split among different protocols worldwide, with one of the most common outside the U.S. being GSM (Global System for Mobile Communication). So far, cellular has not made significant inroads into the smart container world even though there are roaming capabilities and connectivity between different areas of the world.

Although there are dedicated bands for radio LANs (local area networks), and for industrial, scientific, and medical bands in the spectrum above 2,400 MHz and “set asides” designated by the FCC in the U.S. and its counterpart in Japan, barriers to wider use of cellular for smart container use abound. For a start, there are problems similar to those facing RFID with respect to frequencies and bandwidths, protocol challenges, infrastructure network issues related to network gateways, sub-network gateways, towers and base stations.

So far there has been no noticeable progress toward universal acceptance of these cellular technologies as an answer to container communications, especially in light of competing applications and levels of development and sophistication worldwide. Finally, there are fundamental security issues such as interoperability, authentication, tampering, eavesdropping, or access to information that is transmitted in the clear as opposed to being encrypted. In many ways, the cellular communication issues simply mirror those of RFID, thereby limiting its use.

When Does “Smart” Start and Stop?

Much of the current literature on smart containers focuses not on solutions to the problem of security, but on the sensors and communication hardware that are part of the solution. In practice, a truly effective security solution requires a complete system of end-to-end coverage—from a container’s origin to its destination.

The importance of beginning control at stuffing (loading) cannot be overemphasized. It is required by the World Customs Organization, the U.S. Customs Trade Partnership against Terrorism (C-TPAT), and Europe’s new Authorized Economic Operator (AEO) program. Also, the U.S. SAFE Port Act of 2006 defines global supply chain as beginning at a container’s origin and ending at its destination. Its process adds the human element—a vital component that is often eclipsed by preoccupations about technology.

At origin, container systems must include the identification of a party responsible for final inspection of the cargo prior to its dispatch and subsequent international movement. Someone must take responsibility for confirming the cargo on the bill of lading or booking sheet, for activating the smart container system, and for locking the doors. This responsible person must be vetted for his
or her integrity and competence.

Equally, there must be a counterpart at destination, and both parties must be electronically associated with the smart container by a unique identifier in order to complete the system. This can be done with an activation key that is loaded at origin with the bill of lading and booking information. Other data (such as the identity of the supervising and arming agent at origin) then allow the final agent to deactivate the system at destination. The secure electronic key is used to transport and insert the data from the company’s logistics system into the device affixed to the container. When the key is used to activate the system at origin, the data contained in the container device’s memory can be read at almost any time during the voyage through satellite communication.

The activation also allows a smart container to notify appropriate parties of an unauthorized breach or to report the condition of the container. Depending on the sensors used, it could also report the condition of the cargo and even provide off-course alerts on its own hijacking all the way from origin to destination.

In effect, the process becomes the equivalent of a chain of custody. It treats the container as if it were a certified and registered letter. The smart container provides the ability to serve as a third-party record of the transaction recorded automatically by a worldwide call center. It offers an electronic receipt of delivery, accomplished by the opening of the container by an approved and authorized person at the destination. This is provided via another specialized electronic data key usable only with and by an authorized individual at the point of destination. The process exceeds the security of registered mail by offering breach detection not just through the doors, but through any part of the container.

A smart container system, then, is much more than just a locked door. It is a complete system that must:• Electronically identify the authorized personnel stuffing and securing the container, and accept and report information such as container/trailer number and booking data.
  • Detect a breach in any part of the container.
  • Report the breach in real time (or close to real time).
  • Track the container through the supply chain.
  • Identify authorized personnel unsealing container.
  • Be software-friendly to accommodate disparate logistics programs in communicating critical data.

What Is It Worth, and Who Pays?
The short answer is that we all pay for the costs of secure container shipments one way or the other, and shippers and carriers have very few options. The use of in-container security devices is not mandatory anywhere in the world at this time, although it is moving in that direction. It is encouraged in the SAFE Port Act with the “teaser” benefit of special Tier 3 “Green Lane” provisions for companies that use them.

C-TPAT is one such government program. While now codified into U.S. law, C-TPAT is still a volunteer program that allows and encourages companies involved in international trade to become members. By becoming members, the companies must meet security obligations. Current and potential members include: air carriers; sea carriers; rail and truck carriers, including foreign truck carriers; air freight consolidators; U.S. marine ports/terminals; warehouses; U.S. licensed customs brokers; importers; and any manufacturers producing in Mexico and shipping to the U.S.

But it is clear that organizations that volunteer to be members incur significant expenses to do so. For instance, a U.S. importer must mandate and ensure that its foreign suppliers meet the same requirements that it does. The importer must spend money on security measures at its facilities, on security training and education, and on technology. Essentially, the cost burden for security is being shifted to volunteering companies, making the U.S. government’s job easier.

The security requirements are extensive. In March 2005, the following C-TPAT requirements became effective for U.S. importers:
  • Business Partner Requirements: Foreign business partners must meet the same C-TPAT requirements of those of the U.S. importer.
  • Security Procedures: Procedures begin at stuffing the container and include participating in foreign customs administrations’ supply chain programs.
  • Container Security: These criteria include required inspections, ISO container seals, and container storage.
  • Physical Access Controls: Controls are applied to employees, deliveries and visitors, and systems are applied for challenging and removing unauthorized persons, for running background checks, managing investigations, and handling personnel termination procedures.
  • Procedural Security: Security applies to documentation processing, manifest procedures, shipping and receiving, and cargo discrepancies.
  • Security Training and Threat Awareness: These pro-
cedures require security education and the establishment and maintenance of training programs.

- **Physical Security:** A component that addresses fencing, gates and gate hours, parking, building structure, locking devices and key controls, lighting, alarm systems and video surveillance cameras.

- **Information Technology Security:** Addressing password protection and accountability.\(^4\)

In March 2006, U.S. Customs and Border Protection described how the United States’ “Zone of Security” is being pushed back to the point of origin and how participation in C-TPAT “…allows for better risk assessment and targeting, freeing CBP to allocate inspectional resources to more questionable shipments.” The inference seems to be that the private sector should bear the burden of pushing back the security zone in exchange for expedited shipments through U.S. customs (Tier-1 treatment; Tier-2 treatment; and Tier-3, also called Green Lane treatment), for a lower probability of inspections and for having a designated manager at CBP for their account.\(^3\) The problem is that pushing back the border is not Target’s or Home Depot’s duty. It’s the duty of the U.S. Congress and the Administration.

### At a minimum, the federal government should offer tax relief in the form of a tax credit for investments in container security programs.

The benefits to Tier 3 participants may include: the expedited release of cargo in destination ports within the United States during all designated threat levels; further reduction of examinations of cargo; priority for examination of cargo; and further reductions in the risk score assigned pursuant to the CBP’s Automated Targeting System. A recent CBP report says that participants will see average reductions of more than 34 percent in examinations, nearly 30 percent better supply chain visibility, a 22 percent gain in their ability to track orders, and close to 30 percent fewer supply chain disruptions. However, genuine expedited service will rest with the implementation of Green Lanes, which will depend on the use of smart boxes and which should give a return to the shipper or importer.

The catch is this: Green Lanes do not yet exist at U.S. seaports, and in reality, the benefits of that level of C-TPAT membership are few. So far, there really is no incentive for a private company to sign up for C-TPAT when the benefits are not guaranteed but the up-front costs are. Until Congress offers something more than a voluntary program with unreliable benefits, paying for and using a smart container will be an industry decision for industry-recognized benefits. At a minimum, the federal government should offer tax relief in the form of a tax credit for investments in container security programs and for involvement with programs such as C-TPAT. If the U.S. Congress can give a tax credit for railroad track maintenance, it can do the same for support of national security rather than expecting the bulk of the practical effort and investment to fall on private industry’s shoulders.\(^6\)

The increased use of container security systems will ultimately depend on industry’s recognition of the bottom-line benefits and on the existence of real government incentives. The sooner those incentives can materialize, the sooner businesses are likely to see benefits from smart containers.\(^6\)

### Sources:

1 Barchi Peleg-Gillae, Gauri Bhat, and Lesley Sept, Innovators in Supply Chain Security The Manufacturing Institute, Stanford University, July 2006, p. 4.


5 Currently if CBP examines a container, all others listed on the entry are held in the port until the initial inspection is completed. In April 2007, CBP claims to be developing a new procedure for C-TPAT participants that would require only the container(s) targeted for exam to be held, thereby reducing demurrage fees. Under this procedure trusted C-TPAT importers would be allowed to move the remaining containers to their premises, keeping the container(s) and seals intact, until Customs lifted the hold on the entire shipment.

10 Good Reads on Smart Containers

4. “Security Worth the Cost, Of Course!” American Shipper, June, p. 4.