ADVANCING THE REFORM AGENDA ★ REFORM BRIEF

The Reform Institute, October 3, 2007

Containing the Threat: Protecting the Global Supply Chain Through Enhanced Cargo Container Security

Robert W. Kelly, JD

EXECUTIVE SUMMARY

Following a recent series of events that have highlighted disturbing weaknesses in the nation's critical infrastructure (Hurricane Katrina, the Northeast power grid failure, the I-35W bridge collapse, etc.) a welcome dialogue has begun about what we must do to harden our infrastructure against both natural and manmade threats. One of the most critical and poorly understood components within our national infrastructure is the intermodal transportation system – in which the ubiquitous cargo container plays the leading role.

The maritime transportation system is the centerpiece of a global supply chain and accounts for the movement of more than ninety percent of global commerce. Along with bulk cargo and tank ships, the overwhelming majority of goods, raw materials and component parts are shipped in cargo containers that move by sea. The adoption of the container as the principal means of transporting non-bulk cargo has had an unanticipated consequence: as the containerized cargo system has become so efficient and inexpensive, so too has our economic exposure should it be disrupted. Should a weapon of mass destruction (WMD) be detonated in a container, the reliable operation of the world's container terminals and ocean carrier fleets would be one of the casualties. The risk of disruption to world trade rises should the detonation take place in a U.S. port or within the U.S. intermodal transportation system.

The Importance of the maritime domain to our national security cannot be overstated. More than ninety per cent of world commerce is carried by sea.

Should a bomb in a box lead the U.S. government to close our ports and borders even temporarily, it would make clear that the greatest harm for the nation is not what an external force may do to us, but what we are likely to do to ourselves in the aftermath of a terrorist attack. No matter what "Official Washington" may be telling us now – it is unimaginable that it would not result in an immediate shut down of the entire system in a futile search for the "second bomb." Aside from the likely tragic deaths and personal injury, the economic toll of such an event would be catastrophic.

As a nation, we need to focus on hardening every component of our critical infrastructure so that each can absorb a catastrophic event – whether that be a natural disaster, industrial accident or terrorist

The Reform Institute

The Reform Brief is a publication of the Reform Institute, a nonprofit, nonpartisan public policy organization advancing a solutions-based reform agenda.

The Reform Brief examines important public policy issues on the national agenda regarding topics such as government reform, homeland security, energy independence and the environment, economic policy, and immigration reform.

More Reform Institute publications can be found at www.reforminstitute.org.

attack. We must be able to successfully manage a disaster and rapidly return to a state of near normalcy. In the area of container security, Congress recently passed and the President signed a Homeland Security bill calling for 100% screening of U.S.-bound containers in overseas ports within five years. Although this requirement poses significant operational, technological and economic challenges; its successful implementation would go far towards building a more resilient global supply chain.

The purpose of this paper is simple and in keeping with the Reform Institute's overall philosophy. Rather than focusing exclusively on the highlighting of vulnerabilities – and there are many – we focus on practical solutions. As described herein, the adoption of technological solutions such as the "smart container" and the implementation of a workable 100% screening regime for all U.S.-bound containers will help reduce the risk of a serious global disruption to the intermodal transportation system.

BACKGROUND

As a nation, we are still coming to grips with the fact that the war against global terrorism must be fought on many fronts and that it will mirror the cold war in at least one painful aspect. Its course is likely to be measured not in months or years, but in decades; and in the end, unlike the cold war, there is not likely to be a Gorbachev-like, Berlin wall crumbling, series of culminating events. In fact, we may never be able to clearly determine that we have even achieved victory. An important front in this long and difficult campaign will be centered in the maritime domain.

The United States is and, since its birth, has always been a maritime nation. Over the generations we have used the maritime domain as a field of battle, a line of defense, a provider of food, a highway of commerce, a source of energy and a laboratory of science. In recent years it has also become a critical vulnerability, a source of threat and a ready avenue for potential adversaries.

The importance of the maritime domain to our national security cannot be overstated. More than ninety per cent of world commerce is carried by sea. The preponderance of that cargo is carried in containers that move across the globe in a ceaseless stream borne over the seas in larger and larger containerships. Interwoven with this trade are vessels of all sizes carrying bulk cargo, petroleum products, chemicals, automobiles, grain, all manner of goods and raw materials. The overwhelming majority of these vessels are engaged in lawful activity and present no threat to the United States; rather their expeditious entry into U.S. ports is vital to our economy. Therein lies the rub: the terribly difficult task of identifying a tiny number of potential threats from within a large, complex and economically vital system of global commerce. The job of identifying and neutralizing threats – hopefully as far from our shores as possible – is made even more complicated by the fact that whatever we do to harden the global supply chain cannot be done at the expense of the rapid and uninterrupted flow of commerce.

We are an important player in a maritime-based trade regime that is dedicated to the efficient movement of energy products, bulk cargo and some sixteen million containers in this extraordinary ballet that uses the entire globe as a stage. In 2007, approximately 200 million container movements will take place in the world's ports. During the past twenty years we have seen unprecedented growth in containerized freight and the development of a highly efficient global supply chain built on a seamless, ubiquitous, intermodal transportation system. The benefits of such a system are obvious and extensive. The risks are also quite clear.

The maritime transportation system is a vital element in our national critical infrastructure and in the global supply chain so central to our economic viability and national security. Containerized freight occupies a central position within this system. If a weapon of mass destruction were to be delivered to our shores hidden within a container and then detonated, it would have a catastrophic impact.

Aside from the immediate loss of life, physical injury and property damage – all of which could be substantial – there would be a cascading effect that arguably would do greater damage to U.S. power. An event, such as described, would almost certainly result in an immediate and severe disruption in the global supply chain. Notwithstanding assurances from government officials to the contrary, it would be unimaginable to think that there would not be an immediate closure of all our ports in a fruitless search for a presumptive "second bomb." Within weeks, the global intermodal transportation system would be in a shambles and once again we may learn that we should have far greater fear for what we may do to ourselves – when we are frightened – than what any outside force may do to us.

THE CONTAINER

In the 1960s a new way of handling and shipping maritime cargo began to gather steam on the nation's waterfront. Prior to the development of the shipping container, maritime cargo was shipped in two ways – bulk cargo (grain, chemicals, minerals, coal, fuel, etc.) and "break bulk" cargo – mixed cargo (food, raw materials, finished goods, components, etc.) placed on pallets and loaded and removed from ships' holds by crane. The break bulk method had a lot of drawbacks. It was extremely time and labor intensive, highly susceptible to pilferage, breakage and weather factors and involved a highly inefficient system for getting cargo from ports to their ultimate destination. Enter the container. A single container could be offloaded from a container ship directly to a truck chassis and could be out of the port facility gate in a matter of minutes. A container loaded with cargo at a manufacturing site, say in Central China, could now be delivered directly to a wholesaler, retailer or distributor, say in Cleveland, without the container ever having been opened. A container ship at a state-of-the-art port facility can now be loaded or unloaded in a matter of hours – a job that would have taken an equivalent amount of break bulk cargo many days.

The unit of measure within the container trade is the "TEU." This stands for "twenty foot equivalent unit." Although there are many containers that are twenty feet in length, the "standard box" is typically forty feet in length. Thus an 8,000 TEU container ship would likely carry somewhat over 4,000 individual containers. Containers are stacked one on top of another in the cargo area of the container ship until the maximum permissible load has been achieved. They are chained in place to prevent unwanted movement while the ship is at sea and have about 8" of free space between the stacks. A single container ship is likely to carry a wide variety of cargo ranging from running shoes to televisions and pharmaceuticals to furniture. To the casual observer, however, all one can see are stacks and stacks of huge, seemingly identical steel boxes.

The maritime transportation system is an industry that typifies the notion that "time is money." Ship operators have made enormous investments in their ships and crews. Ships are designed to operate at maximum speed while transiting between ports and use sophisticated computer models to select routes having favorable wind, current and weather to maximize both speed and fuel efficiency. Arrivals and departures are timed to coincide with the availability of cranes, crane operators and dock space with ships loading and unloading around the clock. Ship operators can ill afford to have these expensive assets lying idle along a pier or riding at anchor awaiting clearance.

The boom in containerized freight that has developed over the course of the past several decades shows no sign of slowing. The order book for new construction in 2006 showed 95 container ships in the size class between 8,000 and 8,999 TEU and 46 ships with a capacity of 9,000 TEU and over. Although the building of larger and faster ships is on the rise, the number of vessel operators has contracted. Now, about 15 operators control over 70 percent of container ships above 1,000 TEU, or 80 percent of the entire global capacity.[1]

At the same time that there is a surge in the building of larger and faster container ships there is a corresponding surge in the construction, expansion and modernization of port facilities around the globe. Nowhere is this more evident than in China. For example, since 2004, the ocean-going cargo throughput of the Chinese port of Dalian has increased by at least 20 million tons per year and container throughput has grown by 20 percent. In 2006, Dalian's ocean-going cargo throughput exceeded 200 million tons, and the container throughput reached 3.21 million TEU, an increase of 58 percent and nearly 100 percent over that experienced in 2003.

The bottom line is that containerized shipping is now and will continue to be the predominant means of shipping goods and material around the globe. Given that reality, it is incumbent on the United States to ensure that we have maximum visibility into what is in the boxes and where they are.

THE THREAT

Those seeking to move contraband around the globe have long since figured out that one of the safest ways to move illicit items is to hide them, in plain view, within the legitimate stream of commerce. Examples abound. Illicit drugs have been concealed in everything from fence posts to cosmetics; high-end stolen vehicles are often moved from country to country hidden in cargo containers. The 9-11 hijackers accomplished their deadly mission while traveling as ordinary airline passengers. The gravest threat to our national security is a non-traditional one and will not be embodied in a conventional military operation. When the next attack occurs it is likely to arise within an ordinary, routine, unexceptional yet ubiquitous feature of everyday life. There are many theories as to what those might be and we have taken measures, some more effective than others, to increase security around these perceived vulnerabilities. Air passenger security has been greatly increased since 9-11 as has security in and around government facilities, events drawing large crowds, power plants, banks and office buildings and so forth. However, when it comes to ordinariness and ubiquity, there is little that rivals the shipping container.

Anyone who has driven on the northern end of the New Jersey Turnpike and seen the hundreds of containers stacked ten-high less than a few hundred yards from the highway and the runways at Newark airport – and within a mile or two of New York City – will get the idea. Containers are everywhere – traveling down the interstates on truck chassis, on flat-bed rail cars, on barges, in container yards, freight terminals, warehouses and in business parking lots all over the globe. Their ubiquity provides a potential terrorist with a powerful tool. Once a container clears a U.S. port of entry it can be bound for anywhere and is subject to virtually no scrutiny.

CONTAINER SECURITY MEASURES TO DATE

In January, 2001 a bi-partisan panel chaired by former Senators Warren Rudman and Gary Hart called for the creation of a cabinet-level agency to assume responsibility for defending the United States against the likelihood of terrorist attacks in the country. The report states "…A direct attack against American Citizens on American soil is likely…In the face of this threat, our nation has no coherent or integrated governmental structures." The report was received with polite yawns in Washington until September 11th of that year, when every politician, pundit and bureaucrat could not get their hands on it fast enough. In October of 2002, the Council on Foreign Relations issued a follow-up report of a task force again chaired by Senators Rudman and Hart. The report was entitled "America; Still Unprepared – Still in Danger" wherein they observed that "Nineteen men wielding box cutters forced the United States to do to itself what no other adversary could ever accomplish: a successful blockade of the U.S. economy." They noted "If a surprise terrorist attack were to happen tomorrow involving the sea, rail, or truck transportation systems that carry millions of tons of trade to the U.S. every day, the

response would be the same – a self imposed global embargo."[2] Although there have been many improvements over the intervening years – including the establishment of the Department of Homeland Security (DHS) – and the creation of a patchwork of programs to bolster supply chain security; there are still serious gaps and the potential for a reaction-driven shut down of the supply chain still looms large.

Over the course of the past four or so years, the U.S. has launched a variety of programs to enhance supply chain security. It has adopted a methodology based on deploying a "layered system of systems" consisting of multiple, mutually reinforcing, security layers that are believed to reduce the likelihood of a single point of failure. The most prominent programs in this patchwork are discussed below.

The Twenty-Four Hour Advanced Cargo Rule
The rule requires all sea carriers, with the exception of bulk carriers and approved break bulk cargo, to provide proper cargo descriptions and valid consignee addresses twenty four hours before cargo is loaded at the foreign port for shipment to the United States. Prior to this requirement many cargo manifests would simply declare that the container had "Freight All Kind" or "General Merchandise" . . . not very helpful information when seeking to determine if a given container posed some element of risk. Failure to meet the twenty-four hour rule results in a "do not load" message and other penalties.

Automated Targeting System (ATS)
ATS takes manifest information provided in accordance with the twenty-four hour rule and uses a system that integrates enforcement and commercial databases. The system is designed to detect anomalies and determines which cargo is high-risk and should be subject to additional scrutiny. ATS accomplishes this by analyzing the data and rank ordering it based on certain rules and algorithms. Upon reaching certain thresholds, cargo may be targeted for further action by Customs and Border Patrol (CBP), including physical inspection of the container.

Container Security Initiative (CSI)
Under CSI, teams of CBP and Immigration and Customs Enforcement (ICE) personnel are assigned to (currently) fifty-four ports around the world that collectively account for about ninety per cent of the containerized freight destined for the U.S. The program calls for CBP to work with host nation customs officials to examine high-risk containers at foreign seaports before they are loaded on vessels bound for the U.S. The three core elements of CSI are:

- Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.
- Prescreen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
- Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. This technology includes large-scale X-ray and gamma-ray machines and radiation detection devices.

Critics charge, however, that added security provided by CSI is illusory since, in large part, targeting is based on the description of contents provided by suppliers. Statistically, less than one per cent of containers passing through CSI ports ever get scanned and only a tiny fraction of them are ever opened for inspection.

Secure Freight Initiative (SFI)
This is a pilot program designed to test high-volume scanning at six ports in Pakistan, Honduras, Britain, Oman, Singapore and South Korea. Containers arriving at participating ports are scanned with both

non-intrusive radiographic imaging and passive radiation detection equipment placed at terminal arrival gates to screen incoming containers. Relay containers – those being transferred from ship-to-ship – would also be scanned. Sensor and image data concerning U.S.-bound containers will be transmitted in near real-time to the National Targeting Center where it will be combined with other available risk data to improve risk scoring and targeting of high-risk containers; thus enhancing the opportunity to conduct further scrutiny of suspect cargo while still overseas. A side benefit of SFI is that it will probably serve as a good indicator of the practicality of the 100% inspection requirement discussed in detail below.

Megaports Initiative

The initiative provides early detection of possible illicit trafficking of nuclear materials through foreign ports. Under this program, the National Nuclear Security Administration – a "semi-autonomous" agency within the Department of Energy – installs radiation detection equipment at foreign ports to bolster the detection and interdiction capabilities of officials within the partner nations. The program is designed to provide the foreign governments with the ability to screen incoming, outbound and transshipped cargo while posing a minimal threat of delay to port operations. NNSA has identified seventy ports of interest in some thirty-five countries based on the volume of U.S.-bound containers. To date, however, it is only operational in Greece, Bahamas, Sri Lanka, Spain, Singapore and the Netherlands.

Customs-Trade Partnership Against Terrorism (C-TPAT)

C-TPAT is a "public-private partnership" that is designed to strengthen the global supply chain by the voluntary agreement of the private sector program participants to adopt a wide range of security measures. For example, in the area of container and trailer security, members are required to take certain measures to ensure that containers and truck trailers are protected against the introduction of unauthorized material and/or persons. At the point-of-stuffing, containers and trailers must be sealed using an approved "high security" seal and an inspection must be conducted to assure the physical integrity of the box. Other C-TPAT requirements include personnel security, procedural security, information technology security, physical security and security training/threat awareness. C-TPAT is open to a fairly wide range of industries in the trade community including importers, sea, air and land carriers, air freight consolidators, port/terminal operators, foreign manufacturers and warehousing operators. In return for their participation, C-TPAT members are extended certain benefits that reduce the level of scrutiny that participant's shipments are subjected to when entering the United States. As a result of their certification as a C-TPAT member, the risk profile on their shipments is reduced; thus subjecting it to a far lower likelihood of extensive documentary and physical inspection. Additionally, they receive access to FAST lanes on the Canadian and Mexican border and expedited cargo processing at FAST lanes. C-TPAT is built around a self-reporting and self-policing protocol. C-TPAT members are certified by CBP on the basis of self-reported compliance with mandated security measures and are vetted, in part, based on prior history concerning violations and compliance with customs regulations. Critics of C-TPAT, including the GAO, question whether CBP has sufficient procedures and personnel to validate that C-TPAT members are indeed compliant with mandated security measures.

CONTINUING SECURITY GAPS

The above programs are described as a patchwork for good reason. Although to the casual observer it would appear that enormous progress has been achieved in securing the global trade and transportation system; regrettably, this is not necessarily the case. There is little coordination among the various programs, with each marching forward with scarce regard for the other. Uneven

funding among the programs and inflated claims of effectiveness by agency heads and the Administration compound the problem.

In testimony before the Senate Homeland Security and Governmental Affairs Committee on March 28, 2006, Dr. Stephen Flynn of the Council on Foreign Relations and author of the books *America the Vulnerable* and *The Edge of Disaster* provided a chilling scenario for how these various initiatives could be circumvented by a determined terrorist. In Flynn's scenario a container of sneakers manufactured for a name brand company are stuffed in a container in Indonesia. While in route to the port the driver takes a detour and the container is breached – without disturbing the mechanical seal – some sneakers are removed and replaced with a dirty bomb wrapped in lead shielding. A coastal feeder ship carries the container to Jakarta where it is loaded onto an Inter Asia ship for transport to Hong Kong. There it is loaded on a giant trans-Pacific container ship bound for Vancouver. Because the shipment was of a trusted name brand company that was a member of C-TPAT, CSI inspectors in both Hong Kong and Vancouver would not have identified it for further inspection. The nature of the destructive device would also have prevented it from being detected by any radiation portals that it may have passed through. From Vancouver the container is loaded directly on a Canadian Pacific rail car where it is shipped to a rail yard in Chicago. When it reaches a distribution center in the Chicago area, a triggering device attached to the door detonates the bomb.[3]

Flynn points out that in this scenario, aside from the loss of life, injury and potential widespread environmental damage, there are other dire immediate consequences. Since there would be no way to determine where the compromise to security occurred, there would be a presumption that the entire supply chain was compromised and all the transportation nodes and providers would be presumed to present a risk of a follow-on attack. Further, all the existing container and port security initiatives would be compromised by the incident. Governors, mayors and others charged with public safety, along with the American people, would lose faith in the risk management strategy that the government had put in place and would doubtless demand an immediate 100% screening of all cargo entering the U.S.[4] Once again, the United States would have self imposed a global embargo.

100% SCREENING

Although the notion of requiring 100% radiation screening of all U.S.-bound containers is a subject that has been debated for years, the Homeland Security Bill signed into law in August, 2007 transformed the debate from an academic one to reality. Congress, intent on passing a law that embraced the recommendations of the 9-11 Commission, enacted a Homeland Security Bill - that was eventually signed by the President, albeit reluctantly - having a provision calling for radiation screening, within five years, of 100% of U.S.-bound maritime cargo before loading at foreign ports. The Secretary of the Department of Homeland Security is, however, permitted to extend the deadline two years at a time in the event that there are insurmountable technical or other hurdles. In requiring 100% screening, Congress actually stepped out beyond the 9-11 Commission that had only called for an intensified effort to track and screen "high risk" cargo through more practical and sophisticated tactics. The Commission had recommended a layered approach integrating intelligence gathering, risk assessment and the engagement of both foreign governments and the private sector to target potentially dangerous cargo for closer scrutiny.

The Administration, DHS leadership and component agency heads, numerous business groups including the Chamber of Commerce, the National Retail Federation, the International Cargo Security Council and, not surprisingly, shippers all strenuously opposed this component of the bill. They contend that the requirement is beset with problems, not the least of which is the fact that the technology to perform the screening may not exist,

that it is not clear precisely what is to be scanned, that how the cost will be allocated has yet to be addressed and that the process may delay the flow of inbound goods. Some of these arguments have merit; others do not.

TECHNOLOGICAL SOLUTIONS

There are essentially two types of scanning systems used on maritime containers that are currently deployed at ports around the world and at U.S. ports; or which have been deployed on a test basis in various ports. The more widely fielded of the two technologies are radiation portal monitors. They are designed to detect the presence of radioactive material in containers. The second type of scanning equipment is the gamma-ray, which is used to scan the contents of a container for dense material that would indicate the presence of explosives or, more likely, explosives shielded in lead. Both technologies provide for increased security within the supply chain, but still leave substantial vulnerabilities in place.

Portal monitors and gamma-ray machines have their limits. Although they can do a creditable job of addressing two types of threats – they leave other potential threats untouched. These technologies cannot detect the presence of chemical or biological agents. They cannot determine if a container has been breached at some point in time from its stuffing to its final destination and they add little overall value in supply chain visibility or forensics in the event of an actual detonation.

The "smart" container, however, offers the potential to harden the global supply chain by making it a far less attractive target to a wide range of terrorists and trans-national criminals who use the supply chain to traffic in drugs, humans, counterfeit goods, weapons, precious metals, currency, and stolen goods. There are essentially two types of smart containers. One uses radio frequency identification (RFID) tags that are installed within the container and are connected to a sensor that detects when a container door is opened. The second type of system typically uses a more sophisticated suite of sensors that can detect when the integrity of a container is breached and also typically uses satellite communications technology rather than radio frequency to communicate the intrusion.[5]

The RFID system has some significant limitations. It typically only transmits in response to a query from an external transceiver; thus a significant period of time can elapse between the time of the breach and its reporting. Secondly, the ability to detect when a container door is opened does not address the fact that a determined adversary is capable of breaching the integrity of a container through means other than through the door. Finally, these systems typically do not have the capability to provide continuous geo-location information.

A truly "smart' container should have capabilities far beyond this. It should be able to:

- Record the identity of the person supervising the stuffing of the container and arming its security system at its point of origin.
- Provide for electronically capturing trade and manifest data extending from the point and time of departure at origin through its delivery at destination. Data can be drawn from bills of lading, booking confirmation and dray orders and could potentially include information such as:
    - Document number
    - Booking number
    - Shipper/exporter
    - Forwarding agent and license number
    - Location of point of stuffing
    - Date of departure
    - Consignee
    - Notify party
    - Place of receipt by land carrier
    - Ocean carrier
    - Port of loading
    - Location of pier or terminal
    - Port of discharge
    - Declared value
    - Container ID number

  - Gross weight
  - Description of goods.

- Detect a breach anywhere within the body of the container.
- Report the breach in real-time or near real-time and provide a time stamp and geographic position.
- Provide geo-location information throughout its movement through the supply chain, when polled, and provide an automatic position report when it is off its designated route of travel.
- Recognize and record the authorized person opening the container at destination.
- Be adaptable to a variety of different supply chain software packages used by various shippers and carriers.[6]

Smart containers provide both supply chain security and commercial benefits. From a security perspective smart containers provide a significant deterrent to a would-be terrorist and even in the event of a successful attack, the detailed electronic audit trail provided by the smart container will provide a powerful forensic tool. From a commercial standpoint, all manner of transportation providers within the supply chain will benefit from far greater visibility into the movement and status of their cargos.

SUMMARY AND CONCLUSIONS

Notwithstanding the various challenges that face the implementation of a 100% cargo screening system; it is law and it is going to happen. The day for debating the operational, political, economic and technological merits is past. Rather than spend the next five years engaging in a series of delaying tactics or jockeying for position to make the case that a two-year extension is warranted, our nation and this vital global industry need to come together and implement viable technological solutions to supply chain vulnerabilities now. The technology exists today to harden the global supply chain by the adoption of both smart containers and the deployment of radiation screening at those ports that account for the overwhelming percentage of U.S.-bound containers.

As stated above, smart containers have both security and commercial benefits. They remove all question as to whether or not the goods stuffed in the container at the point of origin are indeed the same goods in the same quantity at the point of destination. The smart container generates the electronic equivalent of a receipt that documents contents and evidence of shipping. This data is provided by an electronic key that is accessible only by authorized persons at origin and destination. The smart container provides the shipper and the carrier unprecedented visibility into the location and status of assets and cargo. Most compellingly, smart containers, with their ability to detect a breach anytime and any place and transmit an alert in real-time or near real-time, offer a significant deterrent to anyone desiring to use the container system for the transport of contraband or to use the container as a weapon.

Those who argue that 100% screening is not technologically feasible need to examine a pilot project that has been operational since 2004 in Hong Kong and sponsored by the Container Terminal Operators Association of Hong Kong. At two of Hong Kong's busiest terminals – indeed among the busiest on the planet – every container entering the terminals by truck (moving at 15kph) is subjected to a gamma-ray scan of its contents and a radiation portal to detect and record levels of radiation. Additionally, optical character recognition cameras record the numbers painted on the container's top and sides.[7] All the data – scans, radiation profiles and photographs – are stored in a common database accessible – immediately if warranted – by customs officials.

The Hong Kong group established this system out of self interest. They believed that by conducting 100% screening they reduced the likelihood that a terrorist would put a weapon of mass destruction in a container passing through ***their***

port. The system that they selected allows the inspection to take place while the container is moving and is remote from the terminal itself. It solves the problem of suffering the disruption that occurs when a container is removed from a terminal after being targeted for inspection… only to be returned later. Finally, in the event of a terrorist attack within the supply chain, the Hong Kong terminals would have an impressive audit trail and forensic tool to both assist investigators in a post-event scenario and further would provide strong evidence to argue that cargo originating in their port should not be subject to any sort of post-event embargo. One hundred per cent inspection technology is ready, working and should be deployed without delay.

A final question raised by critics of 100% screening is "Who is going to pay for it?" resulting, in part, from the not surprising failure by Congress to appropriate funds for this requirement. There are a number of ways to fund not only the 100% screening requirement, but to also fund the deployment of smart containers throughout the supply chain. Destination port operators could offer reduced fees to cargo originating in 100% screening ports of origin or alternatively impose fees for failing to implement a 100% screening regimen. Foreign port operators and shippers would soon see a commercial benefit in getting with the program. It has been estimated that the total cost of adopting a 100% screening system and deploying smart containers would likely be between $50 to $100 per container. Even if the final cost approached the upper end of that range, the cost of the average price of consumer goods moved for U.S. retailers would increase by only about .2 percent.[8]

Perhaps the strongest argument for adopting both of these technological solutions is that we would be doing what needs to be done in virtually every component of our nation's vital infrastructure – hardening it to withstand a range of potential threats and giving it the kind of resiliency that will allow it to bounce back from a catastrophic event. Whether we are talking about the power grid, our interstate highway system, river levees, water distribution systems or the supply chain, the same holds true for all. We need to apply the best solutions so that we can respond to the worst; whether the source of the harm is the weather, industrial accidents, natural disasters or the deliberate acts of those who seek to do us harm.

ENDNOTES

[1] *Shipping Statistics and Market Review, June, 2006.*
[2] "The Fragile State of Container Security", Written Testimony before the Senate Governmental Affairs Committee, March 20, 2003, Stephen E. Flynn, PhD., Jeanne J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations.
[3] Testimony before the Senate Homeland Security and Governmental Affairs Committee, March 28, 2006, Stephen E. Flynn, PhD, Jeanne J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations.
[4] Ibid.
[5] The Journal of Commerce online, *Smart Containers and the Chain of Custody,* Traffic World, *February 12, 2007*, James Giermanski, Chairman, Powers International
[6] Cargo Security International, *Is it Safe? February/March 2007, James M. Giermanski*
[7] Flynn, March 20, 2006.
[8] Ibid.

Robert W. Kelly is Senior Advisor to the Reform Institute's Homeland and National Security Center. He is also the Managing Partner of CenTauri Solutions, LLC, a professional services firm that specializes in high-end consulting and technical services for the public and private sectors.