COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10065
Tel 212 434 9400 Fax 212 434 9800

"Overcoming the Flaws in the U.S. Government Efforts to Improve Container, Cargo, and Supply Chain Security"

Written Testimony before

a hearing of the

Homeland Security Appropriations Subcommittee,
Committee on Appropriations,
United States House of Representatives

on

Container, Cargo and Supply Chain Security – Challenges and Opportunities

by

Stephen E. Flynn, Ph.D.
Jeane J. Kirkpatrick Senior Fellow in National Security Studies
Council on Foreign Relations
sflynn@cfr.org

Room 2359
Rayburn House Office Building
Washington, D.C.

10:00 a.m.
April 2, 2008

"Overcoming the Flaws in the U.S. Government Efforts to Improve Container, Cargo, and Supply Chain Security"

by
Stephen E. Flynn, Ph.D.
Jeane J. Kirkpatrick Senior Fellow
for National Security Studies

Chairman Price, Ranking Member Rogers, and distinguished members of the House Appropriations Subcommittee on Homeland Security. Thank you for inviting me to provide an assessment of the current U.S. Government efforts to improve container, cargo, and supply chain security. This is a complex issue with enormous stakes for our economy and national security. As such, it is vitally important that U.S. programs, whose aims are to address this issue, receive the kind of careful oversight this subcommittee is providing today.

Today the subcommittee will hear testimony from Customs and Border Protection and the Domestic Nuclear Detection Office. These two agencies have been assigned a leadership role in devising the programs and deploying the tools for managing the risk that global supply chains may be compromised by terrorists intent on using the intermodal container to smuggle nuclear weapons or materials into the United States. To date, the leaders of these agencies have expressed confidence that the strategy they are employing against this risk is up to the task. While CBP and DNDO deserve good grades for effort, given the complexity of the issue and the relatively modest resources the Bush Administration has applied toward it, no one should be surprised that we are closer to the starting line than the finishing line when it comes to managing this risk.

Let me begin by offering some perspective on the resource issue. On March 5, 2008, I testified before the House Oversight Subcommittee on Foreign Affairs and National Security on the huge imbalance between the homeland security budget for responding to the more probable nonmissile threat to the United States vis-à-vis the $12.3 billion the Bush Administration has requested to support research for developing ballistic missile defense in 2009. This latest missile defense request is on top of the more than $120 billion taxpayers have already spent since 1985 to develop a system conceived at the height of the Cold War to deal with the massive Soviet arsenal of nuclear-tipped intercontinental missiles. The consensus among security experts both inside and outside the U.S. government is that the most likely scenario for an attack involving a nuclear weapon on U.S. soil is one that does not involve a long range missile. Instead al Qaeda or a future adversary will smuggle the weapon or more likely the materials for assembling the weapon inside the United States. Smuggling has three advantages over a missile: it is far easier, lower cost, and anonymous. Yet the combined proposed budgets for funding all the domestic and international maritime and port of entry interdiction efforts pursued by the Coast Guard, Customs and Border Protection, and DNDO is only one-half of the annual budget the White House wants for missile defense.

Despite the limited resources involved, the U.S. Department of Homeland Security has generally been overstating what they have been accomplishing when it comes to cargo security. Their efforts fall short on four counts:

(1) The data that CBP relies on for identifying suspicious cargo is too unreliable to support the "risk management" methodology it employs, although its new proposed "10+2" regulation is a positive step towards addressing this problem.

(2) The Container Security Initiative arrangement now in place in 58 ports around the world can support only a tiny percentage of pre-loading inspections of U.S.-bound containers that are evaluated as suspicious. This means that the majority of the containers that CBP's targeting algorithm identifies as sufficiently anomalous to warrant an examination will continue to be carried out primarily upon arrival in the United States, potentially placing the U.S. port and the adjacent community at risk.

(3) The radiation monitors that have been deployed in U.S. ports to evaluate the risk that cargo may be carrying nuclear weapons or materials are ineffective in detecting shielded highly enriched uranium (HEU), a nuclear weapon, and a shielded radiation dispersal device (i.e., "dirty bomb"). The high profile DHS has given to the deployment of this equipment has created a false sense of security.

(4) The U.S. government lacks a credible plan for managing a major security breech in the global supply chain. This places the intermodal transportation system at risk of widespread economic disruption generating tens of billions of dollars in losses, and potentially endangering lives as the shipments of critical time-sensitive goods such as medical supplies and defense-related materials are interrupted.

The current U.S. container security programs are inadequate for addressing the complexity of the challenge or for the stakes involved in managing the global risk that supply chains may be compromised by terrorists. The way ahead must involve a far more vigorous effort by the U.S. government to provide incentives for private sector participants to develop robust means to monitor and validate the flow of legitimate cargo and to closely partner with the U.S. government and other governments in managing security incidents.

THE LIMITS OF AN HONOR SYSTEM

The process for calculating risk that is currently used by CBP begins with an analysis of the cargo manifest that an ocean carrier provides about shipment that has been accepted for transport to the United States. This cargo manifest is provided to CBP by the carrier based on information provided by a shipper about the cargo it has contracted for transport. Since the container is sealed, an ocean carrier is in no position to confirm the veracity of the declarations it receives from its customers. Essentially, it is an honor system.

Once a containerized shipment triggers an alert, CBP can access a variety of databases to get an impressive array of additional information to help determine where a container should be selected for examination. However, except in very rare instances when there is specific intelligence, the alert mechanism relies on the truthfulness of the data provided by an importer and ocean carrier.

Unfortunately, some shippers are not entirely forthcoming with their descriptions of the cargo they are shipping. This reality was graphically highlighted with disastrous consequences on March 21, 2006. Per the photos below, the M/V HYUNDAI FORTUNE, a large ocean-going containership, transiting from Asia to Europe via the Suez Canal, had a catastrophic fire off the Gulf of Aden, 60 miles south of the coast of Yemen. Efforts to contain the fire failed and the crew abandoned ship. Ultimately the ten-year old ship was sold for scrap.

The cause of the fire is believed to have been a container loaded with petroleum-based cleaning fluids stowed near the engine room. The shipper failed to indicate the hazardous nature of this shipment to the HYUNDAI FORTUNE, undoubtedly to avoid the special handling fees associated with transporting hazardous materials. Around 10 percent of container cargo worldwide comprises hazardous goods, but as the M/V HYUNDAI FORTUNE incident makes clear, not every shipper or consignee chooses to ensure that a carrier is adequately notified.


APL
NOL
APL
MOL
APL
APL
APL


A I

The second important component of CBP's decision to examine a shipment involves a determination as to whether the importer is a "known shipper." The underlying assumption of the known shipper program is that past performance can serve as a predictor of future results. That is, if an importer or transportation provider has an established track record of being engaged in legitimate commercial activity and playing by the rules, CBP assumes they will be less likely to be compromised by terrorist. Since 9/11, the agency has built on that model by extracting a commitment from shippers to follow voluntary supply chain security guidelines outlined in the Customs-Trade Partnership Against Terrorism (C-TPAT). As long as there is not specific intelligence to tell inspectors otherwise, shipments from C-TPAT companies are viewed as presenting little risk.

The problem with this approach is that what may have made sense for assessing the risk of crime or regulatory noncompliance does not automatically translate to combating determined terrorists. When it comes to warding off criminals, private companies can indeed put in place meaningful security safeguards that can deter criminals from exploiting legitimate cargo and conveyances for illicit purposes. This is because good internal controls raise the risk over time that criminals that try and penetrate the operations of a legitimate company will be caught and their illicit enterprise will be shut down. Organized crime groups want to maximize their profits by sustaining ongoing conspiracies. As such they tend to gravitate towards the places where the controls are weakest, and law enforcement's reach is only episodic.

But a terrorist attack involving a weapon of mass destruction differs in three important ways from organized criminal activity. First, it is likely to be a one-time operation and most private company security measures are not designed to *prevent* single event infractions. Instead, corporate security officers try to detect infractions when they occur, and conduct credible investigations after the fact that support imposing sanctions in order to foster a culture of compliance within the workplace. This approach tends to work in deterring most employees from being drawn into an ongoing criminal enterprise. However, it is not up to the task of detecting and preventing a situation where a terrorist organization seduces or intimidates an employee with a one-time offer or threat that he or she cannot refuse.

Second, terrorists are likely to find it particularly attractive to target a legitimate company with a well-known brand name precisely because they can count on these shipments entering the United States with a only a cursory look or no inspection at all. It is no secret which companies are viewed by U.S. customs inspectors as "trusted" shippers. Many companies who have enlisted in C-TPAT have advertised their participation in press releases or with postings on their website. In public speeches, senior U.S. customs officials have singled out several large companies by name as model participants in the program. All a terrorist organization need do is to find a single weak link within a "known shipper's" complex supply chain, such as a poorly paid truck driver taking a container from a remote factory to a loading port. They can then circumvent the mechanical door seal and gain access to the container in one of a half-dozen ways well-

known to experienced smugglers. Since inspectors view past performance as the primary indicator of current and future compliance, as long as the paperwork is in order, the compromised cargo container almost certainly will be cleared to enter a U.S. port without anyone ever looking at it.

There is third important reason why terrorists would be more willing than criminals to exploit the supply chains of well-established companies. By doing so, they can count on generating far greater economic disruption. This is because once a dirty bomb arrives in the United States via a known and trusted shipper, the risk management system that customs authorities are relying on will come under withering scrutiny. In the interim, it will become politically impossible to treat cross-border shipments by other trusted shippers as low risk. When every container is assumed to be potentially high risk, everything must be examined which translates into putting the intermodal transportation system into gridlock.

PUSHING THE BORDERS OUT:

I have long been an advocate of developing measures for securing the global supply chains that emphasize controls that begin where goods originate and examinations conducted at the port of loading instead of the port of arrival. Shortly after September 11, 2001, I had the opportunity to meet with Robert Bonner, the then Commissioner of U.S. Customs, to discuss a *Foreign Affairs* article I had written in 2000 entitled, "Beyond Border Control." What was to become the Container Security Initiative grew out of those conversations.

Today Customs and Border Protection has Container Security Initiative arrangements in place in 58 ports around the world. Under this protocol, CBP can ask that their overseas counterparts conduct inspections of targeted containers before they are loaded on a U.S.-bound container ship. This approach both protects the ship from a HYUNDAI FORTUNE-like incident, and the U.S. port where the container is destined.

In practice, CSI teams have been able to inspect only a fraction of a percent of U.S.-bound cargo in busy ports of loading like Singapore and Hong Kong. There are three reasons for this. First, since the inspections are conducted by the host-country's personnel, CBP has to be careful not overburden these inspectors with examinations of U.S.-bound cargo that often is done at the expense of these foreign inspectors completing their own work. The overwhelming majority of containers that CBP targets for examination turn out to be benign due to the limits of their targeting algorithm. Requests for lots of examinations that prove to be false alarms endanger the support for CSI by the host country.

The second reason why CBP is extremely conservative about its port-of-loading requests is that they can be very disruptive to port terminal operations. The decision to examine a container overseas is made after the ocean carrier provides information about that container 24 hours in advance of loading. For larger container ships, that loading process can take 18 hours or more. CBP's decision to have a container inspected before loading

places the shipment at risk of missing its voyage with all the resultant disruption to the importer's supply chain. This is because the container often must be physically removed from the stacks of containers within the terminal and transported to the inspection facility managed by the overseas customs inspectors. If CBP routinely asked that as little as 1-2 percent of U.S.-bound containers be subject to examination before loading, it would likely completely overwhelm the inspection facility. The result would be major delays in shipments. For the overseas marine terminal operator, being directed to routinely locate and remove U.S.-bound boxes from their stacks shortly before scheduled loading can be enormously disruptive to yard operations. These terminals are modern wonders of efficiency. A request to remove a container from their yard is like interrupting a well-honed assembly line.

These challenges associated with conducting CSI examinations at the port of loading translate into inspections being the exception to the rule. The vast majority of containers that CBP deems to be anomalous enough to warrant an inspection sail to the United States and are inspected upon arrival. CBP has been managing this by essentially creating a two-tier system where only containers it judges to present a very high risk are examined overseas. The problem with this approach is that the targeting system is based almost entirely on anomaly detection and not on specific intelligence. CBP does not have a reliable tool for distinguishing between shipments that are very high risk versus "just" high risk.

Waiting until a container arrives in a U.S.-port before it is examine undermines one of the most important advantages of CSI; i.e., protecting the U.S. port complex and its community from the risks associated with a WMD entering that port. Should a WMD arrive in a U.S. port and be triggered before or during an inspection, it places critical infrastructure and potential the lives of hundreds of thousands of people at risk. Should it be discovered without being triggered, it will likely shut down port operations for an extended period of time while it is cleared and labor is reassured that it is an isolated incident. Should this be a major port complex such as Los Angeles/Long Beach or Seattle/Tacoma, the resultant disruption to supply chains could reverberate throughout the national economy.

THE LIMITS OF RADIATION DETECTION TECHNOLOGY

DHS's "last line of defense"—radiation monitors along our borders and within our seaports—is critically flawed. In the April 2008 issue of *Scientific American*, Thomas Cochran and Matthew McKinzie document what has been long understood by the scientists who understand the physics of radiation detection—that the radiation detectors will only work for unshielded nuclear materials. Since nuclear weapons are shielded by design, they are unlikely to be detected. Highly Enriched Uranium (HEU), the essential ingredient in constructing a nuclear weapon is difficult to detect even in its natural state because it gives off so little radioactivity. As Cochran and McKinzie outline, it requires as little as 1 mm of lead shielding around a canister filled with enough HEU to construct a crude nuclear weapon to avoid detection by the radiation portal technology that DHS has recently deployed within U.S. ports. More lead shielding would be required to avoid

detection of a dirty bomb made with commercially-available nuclear materials, but it is likely that a terrorist intent on smuggling such a weapon into the United States would make such an investment.

THE MORNING AFTER PROBLEM

On March 28, 2006, I outlined the following scenario at a hearing on container security before the Senate Permanent Subcommittee on Investigations:

> A container of athletic foot wear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.
>
> The driver takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship which typically carry 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ships goes to Hong Kong where it is loaded on a super-container ship that carriers 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. Because it originates from a trusted-name brand company that has joined the Customs-Trade Partnership Against Terror, the shipment is never identified for inspection by the Container Security Initiative team of U.S. customs inspectors located in Vancouver. Consequently, the container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a railyard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.
>
> There would be four immediate consequence associated with this attack. First, there would be the local deaths and injuries associate with the blast of the conventional explosives. Second, there would be the environmental damage done by the spread of industrial-grade radioactive material. Third, there would be no way to determine where the compromise to security took place so the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Fourth—and perhaps most importantly—all the current container and port security initiatives would be compromised by the incident.
>
> In this scenario, the container originated from a one of the 5,800 companies that now belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been certified by their host nation as compliant with the post-9/11 International Ship and Port Facility Security (ISPS) Code that came into effect on 1 July 2004. Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors in Hong Kong or Vancouver. Nor would it have

> been identified by the radiation portal. As a consequence, governors, mayors, and the American people would have no faith in the entire risk-management regime erected by the administration since 9/11. There will be overwhelming political pressure to move from a 5 percent physical inspection rate to a 100 percent inspection rate, effectively shutting down the flow of commerce at and within our borders. Within two weeks, the reverberations would be global. As John Meredith, the Group Managing Director of Hutchison Port Holdings, warned in a Jan 20, 2004 letter to Robert Bonner, the former Commissioner of the U.S. Customs and Border Protection: **". . . I think the economic consequences could well spawn a global recession – or worse."**

Today, the U.S. government still does not have a contingency plan for managing the aftermath of this scenario, even though Congress has mandated DHS develop one. In June 2007, Secretary Chertoff rolled out "The Strategy to Enhance International Supply Chain Security" that includes a chapter that outline a response and recovery plan in the aftermath of a major security incident involving a U.S. port. The plan makes no mention of coordination with overseas port authorities and marine terminal operators, ocean carriers, or even our neighbors in Mexico and Canada. Sixty percent of the world's maritime containers are currently at sea. That translates into 10-12 days of shipping traffic underway in the Pacific Ocean and 8-10 days of traffic in the Atlantic Ocean right now. Many of these container ships are post-Panamax which means that they can only be received at the largest seaports and cannot be rerouted. A response and recovery plan that identifies no mechanism to directly engage the global maritime community is not truly a response and recovery plan.

THE PATH FORWARD:

In short, the current container security initiatives have serious shortcomings that do not adequately address the important national security and economic stakes associated with the vulnerability of global supply chains. The challenge of managing the threat that our adversaries might target the United States with a nuclear weapon is not so much tied to our seaports and U.S. borders as it is global supply chains that now largely operate on an honor system because the standards are so nominal. No port operator or border inspector really knows what is in the containers that pass through their facilities and the radiation portal technology currently being deployed at U.S. borders and overseas can be evaded by placing readily available shielding around a weapon or nuclear material. If—when—an attack occurs, the resulting disruption to our society and the national and world economy will be far greater than any of the direct consequences of the incident.

In charting a way forward, it is essential to be mindful of the extent to which private companies and our trade partners have an enormous stake in how we approach the challenge of container, cargo, and supply chain security. The conventional wisdom that security within the global transportation and logistics system is more of a public sector responsibility than a private sector one is wrong. This conventional wisdom persists in no small part because Congress and U.S. enforcement agencies want to be in the driver's seat in managing the security imperative. In practice this translates into "public-private" partnerships involving the public sector setting the requirements and the private-sector being asked to cheerfully embrace the costs of complying with them.

This process needs to be reversed. For the intermodal transportation industry and companies with supply chains that rely on the industry, cargo and container security has become an important business continuity risk. They must be provided with the incentives for taking the lead in developing solutions that manage that risk while government plays a support role.

An example of this is a recent effort by the Port of Los Angeles to reach out to Hutchison Port Holdings, the largest terminal operator in the world, to develop a joint port industry effort to improve container security. Specifically, the Port of Los Angeles is interested in finding a way that terminal operators might invest in and maintain active and passive scanning equipment to examine the contents of containers as they enter their yard. The idea is that if these images could be routinely collected by the terminal operator, when government authorities want to examine the contents of a container, these officials could "pull the bits, instead of pulling the box." That is, inspectors could look at the images of the targeted containers collected by the terminal operators. In the vast majority of the cases the images would reveal there is no dense material and therefore there is no risk that the container is carrying a nuclear weapon or shielded material. These containers could then be immediately cleared for loading without their having to be removed from the stacks. Everyone wins. The terminal operator benefits by minimizing the risk of its yard will be disrupted by these inspections. The ocean carrier benefits by having no disruption to its loading plan. The importer benefits by not having the risk that its container will miss the voyage. Finally, CBP benefits by being able to conduct more inspections under the CSI protocol than the current circumstances allow.

In the end, global networks rely on trust to operate. The private sector must take the lead in developing the systems that sustain that trust. The public sector must be a willing partner in such efforts.

Thank you and I look forward to responding to your questions.

Stephen Flynn is the Jeane J. Kirkpatrick senior fellow for National Security Studies at the Council on Foreign Relations. He is the author of the The Edge of Disaster: Rebuilding a Resilient Nation (Random House, 2007) and America the Vulnerable (HarperCollins, 2004). Dr. Flynn is a Consulting Professor at the Center of International Security and Cooperation at Stanford University; a Senior Fellow at the Wharton School's Risk Management and Decision Processes Center at the University of Pennsylvania; and a member of the Marine Board of the National Research Council. He spent twenty years as a commissioned officer in the U.S. Coast Guard, was awarded the Legion of Merit, and retired at the rank of Commander. During his time on active duty he had two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issues on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.