COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875

"The Limitations of the Current U.S. Government Efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD and a Proposed Way Forward"

Written Testimony before

a hearing of the

Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

on

"Neutralizing the Nuclear and Radiological Threat:
Securing the Global Supply Chain"

by

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies
sflynn@cfr.org

Room 342
Dirksen Senate Office Building
Washington, D.C.

9:30 a.m.
March 28, 2006

"The Limitations of the Current U.S. Government Efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD and a Proposed Way Forward"

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

Chairman Coleman, Senator Levin, and distinguished members of the Permanent Subcommittee on Investigations. I am honored to appear before you again this morning, this time alongside Governor Tom Kean, to discuss the vital issue of nuclear smuggling and supply chain security. At the outset, Mr. Chairman, I want to thank you for the outstanding leadership you have been providing in both raising the profile and advancing practical approaches to this complex challenge. You have been hard at work on this issue long before the Dubai Ports World controversy made the issue of port and container security a hot-button issue here in Washington. I also want to commend the work of Ray Shepherd and Brian White of your staff for their tireless oversight of the activities of the U.S. government on these issues. I would count Mr. Shepherd and Mr. White along with Kathleen Kraninger and Jason Yanussi who are on the staff of the Senate Homeland Security and Governmental Affairs committee, as four of the most knowledgeable individuals on supply chain and container security in Washington.

As I will outline below, the Government Accountability Office is largely on the mark in highlighting a number of serious shortcomings in the design and execution of the radiation detection programs being pursued by the Department of Energy and the Department of Homeland Security. However, before getting into the particulars about what are the limits of these programs and outlining some recommendations for next steps, I think it important to review the nature of the terrorist threat as it relates to this issue.

Let me share with you the terrorist scenario that most keeps me awake at night that I recently shared with the House Armed Services Committee. This scenario has been informed by insights provided to me by Gary Gilbert, the Chairman of the Corporate Security Council and Senior Vice President for Hutchison Port Holdings (HPH) who will be testifying before you on Thursday, March 30th.

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."**

In short the stakes are enormous. But there are four factors associated with the scenario that I just laid out that usefully informs the focus of this hearing. First, the threat is not so much tied to 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. Second, no transportation provider, port operator, or border inspector really know what are in the containers that pass through their facilities and the radiation portal technology currently being deployed at U.S. borders and as a part of the Second Line of Defense and Megaports programs can be evaded by placing light shielding around a weapon. Third, private companies must be a part of the solution since they have huge investments at stakes. Fourth, the scenario I just laid out involved Vancouver as the offload port in North America, highlighting that the challenge of securing global supply chains can involve both port security and border security measures simultaneously.

I believe that we are living on borrowed time when it comes to facing some variation of the scenario I have just laid out. This is because both the opportunity for terrorists to target legitimate global supply chains remain plentiful and the motivation for doing so is only growing as jihadis gravitate towards economic disruption as a major tactic in their war with the United States and the West. Let me elaborate on this latter point.

The primary conclusion that I reached in researching my book, *America the Vulnerable*, is that Americans and the West much assume that our most critical infrastructures that underpin our economy will become the targets of choice for terrorist groups like al-Qaeda. This perspective runs contrary to the longstanding view of terrorism that has held that terrorists are mainly interested in symbolic and spectacular acts of violence that kill lots of people. I point to the attacks on the London public transit system on July 7, 2005, to substantiate my thesis. On that day, suicide bombers simultaneously set off their explosives in subway cars that were in dark tunnels resulting in far fewer deaths than had those same suicide bombers gone to Buckingham palace during the changing of the guard. Further, an attack on a public event would have generated far more dramatic images since there would have been plenty of cameras on hand to capture the destruction and resultant mayhem. But the goal of the London terrorists appears to have been not so much about random killings of innocent civilians as it was an attempt to dissuade Londoners from using their mass transit system, thereby crippling the city economically.

This trend towards economic targeting has been growing in Iraq as well. Beginning in June 2003, Iraq's energy sector became a primary target for insurgents. By mid-July 2005 nearly 250 attacks on oil and gas pipelines had cost Iraq more than $10 billion in loss oil revenue. Successful attacks on the electrical grid has kept average daily output at 5 to 10 percent below the prewar level despite the $1.2 billion the United States has spent too improve Iraqi electrical production. To be sure, there is amble evidence that the war in Iraq has been attracting foreign insurgents and al Qaeda sympathizers to Baghdad versus to Main Street. However, this is likely to prove to be a short-term reprieve that poses a longer-term danger as insurgents become increasingly skilled at targeting critical infrastructure.

Against this strategic backdrop, I believe there remains too little appreciation within the U.S. government that global supply chains and the intermodal transportation system that supports them remains a very vulnerable critical infrastructure to mass disruption. Instead, U.S. border agencies and the national security community have been looking at supply chains as one of a menu of smuggling venues. Some agencies like the Coast Guard and the Office of Naval Intelligence has argued that a weapon of mass destruction is more likely to be smuggled into the United States on a fishing vessel, ocean-going yacht, or a bulk cargo vessel, rather than in a container. This is probably an accurate assumption in the case of a nuclear weapon. A nuclear weapon would be such a high-value asset to a terrorist organization that they would be unlikely to surrender custody of it to unwitting third parties to transport it. But the opposite reason applies to a "dirty bomb" which is more commonly referred to by national security experts as a "weapon of mass disruption" because its lethality is fairly limited, a factor primarily of the conventional explosives with which it is made. The radioactive material contained in the bomb would create costly environmental damage and potentially some long term health risks for those who were exposed, but not immediate deaths. The fact that a "dirty bomb" is suited for *disruption* makes it an ideal weapon to set off within the intermodal transportation system, precisely because it would generate the kinds of consequences that my scenario portends.

For the foreseeable future, the material to make a dirty bomb will likely be available throughout the international community despite even stepped-up counter-proliferation. This is because the radioactive materials that can be used in the construction of these weapons are becoming more widely available as sophisticated medical and engineering equipment are purchased and used throughout the international community. As Gene Aloise of the Government Accountability Office will testify to in the next panel, according to the International Atomic Energy Agency, between 1993 and 2004, there were 662 confirmed cases of illicit-trafficking in nuclear and radiological materials worldwide, over 400 of which involved radioactive materials that could be used to produce a radiation dispersal device or "dirty bomb." These materials have been finding their ways to black markets and will continue to do so.

It is against this threat backdrop that we should evaluate the effectiveness of U.S. government programs who aim to confront this threat.

The possibility that terrorists could compromise the maritime and intermodal transportation system and global supply chains has led several U.S. agencies to pursue initiatives designed to manage this risk. The U.S. Coast Guard chose to take primarily a multilateral approach by working through the London-based International Maritime Organization to establish new international standards for improving security practices on ocean-going vessels and within ports, called the International Ship and Port Facility Code (ISPS). As of July 1, 2004, each member state was obliged to certify that the ships that fly their flag or the facilities under their jurisdiction are compliant. The Coast Guard also requires that ships destined for the United States provide a notice of their arrival a minimum of 96 hours in advance to include a description of their cargoes and a crew and passenger list. The agency then assesses the potential risk the vessel might pose and if the available intelligence indicates a pre-arrival boarding might be warranted, it arranges to intercept the ship at sea or as it enters the harbor in order to conduct an inspection.

The U.S. Customs and Border Protection Agency (CBP) has pursued a mix of unilateral, bilateral, and multilateral approaches. First, U.S. customs authorities mandated that ocean carriers electronically file cargo manifests outlining the contents of containers destined for the United States 24 hours in advance of their being loaded in an overseas port. These manifests are then analyzed against the intelligence and other databases at CBP's new National Targeting Center to determine if the container may pose a risk. If the answer is yes, it will likely be inspected overseas before it is loaded on a U.S.-bound ship under a new protocol called the Container Security Initiative (CSI). As of March 2006, there were 43 CSI port agreements in place where the host country permits U.S. customs inspectors to operate within its jurisdiction and agrees to conduct pre-loading inspections of any containers targeted by them.

Decisions about which containers will *not* be subjected to an inspection are informed by an importer's willingness to participate in another post-9/11 initiative known as the Customs-Trade Partnership against Terrorism (C-TPAT). C-TPAT importers and transportation companies voluntarily agree to conduct self-assessments of their company operations and supply chains and then put in place security measures to address any security vulnerabilities they find. At the multilateral level, U.S. customs authorities have worked with the Brussels' based World Customs Organization on establishing a new non-binding framework to improve trade security that all countries are being encouraged to adopt.

In addition to these Coast Guard and Customs initiatives, the U.S. Department of Energy, Department of State, and Department of Defense have developed their own programs aimed at the potential weapons of mass destruction threat. They have been focused primarily on developing the means to detect and intercept a "dirty bomb" (a conventional explosive device that contains radioactive materials used in commercial applications), the fissile ingredients such as plutonium and highly-enriched uranium used in the construction of a nuclear weapon, and a nuclear weapon itself. The Energy Department has been funding and deploying radiation sensors in many of the world's largest ports as a part of a program called the Megaport Initiative. These sensors are designed to detect radioactive material within containers while trucks drive past them. The State Department is spearheading the Export Control and Related Border Security Assistance Program that includes providing equipment and training for border control agencies. Department of Defense has undertaken a "Proliferation Prevention Initiative" that involves obtaining permission from seafaring countries to allow specially trained U.S Navy boarding teams to conduct inspections of a flag vessel on the high seas when there is intelligence that points to the possibility that smuggled nuclear material or a weapon may be part of the ship's cargo.

Finally, in September 2005, the White House has weighed in directly on container security as a part of its new "National Maritime Security Strategy". The strategy creates an interagency process to oversee the development of eight supporting plans. These include an "International Outreach and Coordination Strategy," a "Maritime Transportation System Security Plan," and a "Maritime Infrastructure Recovery Plan." The stated objective of the strategy and these plans is to "present a comprehensive national effort to promote global economic stability and protect legitimate activities while preventing hostile or illegal acts within the maritime domain."

On its face, this vast menu of U.S. government initiatives since 9/11 suggests substantial progress is being made in securing the global trade and transportation system. Unfortunately, all this activity should not be confused with real capability. For one thing, the approach has been a piecemeal one, with each agency pursuing its signature program or programs with little regard for the other initiatives. There are also vast disparities in the resources that the agencies have been allocated. But more problematic are some of the questionable assumptions about the nature of the terrorist threat that underpin these programs. Further, in an effort to secure funding and public support, agency heads and the White House have oversold the contributions these new initiatives are making towards addressing a very complicated and high-stake challenge. Against a backdrop of inflated and unrealistic expectations, the public will be highly skeptical of official assurances in the aftermath of a terrorist attack involving the intermodal transportation system. Absent change, in the scramble for fresh alternatives to reassure an anxious and angry citizenry, the White House and Congress are likely to succumb to the political pressure to impose draconian inspection protocols that will dramatically raise costs and the disrupt the cross-border trade flows.

The new "risk management" programs advanced by the Customs and Border Protection Agency (CBP) are especially vulnerable to being discredited should terrorist succeed at turning a container into a poor-man's missile. Before stepping down as Commissioner in late-November 2005, the agency's head, Robert Bonner, maintained in public speeches and in testimony before Congress that his inspectors were: "inspect[ing] all high risk cargo containers." Implicit in that assertion is that Americans should be confident that the intelligence and the analytical tools that supported his agency's targeting system could be counted upon to pinpoint the small universe of containers that might present a risk. As such, routinely allowing 95 percent of containerized shipments to enter the United States without any physical examination should not be a source of concern.

Former-Commissioner Bonner is correct in identifying that statistically, only a tiny percentage of containers pose any potential security risk. However, the devil is in the details of how to identify just where the needles might lie within a huge haystack. Unfortunately, CBP's risk-management framework is not up to that task. The fact is that there is very little counter-terrorism intelligence available to support the agency's targeting system. That leaves customs inspectors to rely primarily on their past experience in identifying criminal or regulatory misconduct to determine if a containerized shipment might potentially be compromised for nefarious purposes. This should not inspire confidence given the fact that the Government Accountability Office (GAO) in testimony before the May 2005 hearings of this Committee, and the U.S. Department of Homeland Security's own Inspector General have documented glaring weaknesses with the methodology, underlying assumptions, and execution of customs targeting practices.

Prior to 9/11, the cornerstone of the risk assessment framework used by customs inspectors was to identify "known shippers" that had an established track record of being engaged in legitimate commercial activity and playing by the rules. Since 9/11, the agency has built on that model by extracting a commitment from shippers to follow the supply chain security practices 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 combating crime 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. So all a terrorist organization need do is to find a single weak link within a "trusted" 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 the 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 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.

The International Ship and Port Facility Security (ISPS) code will only contribute to the problem of managing the aftermath of a terrorist attack involving an established importer. This is because all containers arriving in a U.S. port today are being handled by marine terminals and are being carried aboard vessels that have been certified by their host government as compliant with the code. There are no exceptions because if the loading facility or ship were not so certified, it would be denied permission by the U.S. Coast Guard to enter a U.S. port. Accordingly, the credibility of the ISPS code as a risk management tool is not likely to survive the aftermath of a terrorist attack involving a maritime container.

Since the container security initiatives that have been implemented by the Coast Guard and Customs and Border Protection Agency after 9/11 are not posing a meaningful barrier to determined terrorists, presumably one could look to the radiation sensors being deployed by the U.S. Department of Energy to provide a meaningful deterrent. Alas, the technology currently being deployed around the world as a part of the Second Line of Defense and Mageport programs is not up to the task of detecting a nuclear weapon, a lightly shielded "dirty bomb," or highly enriched uranium. This is true not simply because there are problems at many foreign jurisdictions in keeping the detection equipment properly calibrated and in working condition as will be outlined in Mr. Aliose's testimony. But there is a more basic problem which is that nuclear weapons give off very little radioactivity since they are extremely well-shielded so that they can be readily handled. In the case of a "dirty bomb"—as in the scenario I outlined at the start of my testimony—a terrorist who obtained or manufactured a dirty bomb is likely to take the necessary precaution of placing it in a container lined with lead. The result will be that even a properly calibrated radiation sensor is unlikely to be able to detect the very low levels of radioactivity to register an alarm. Finally, highly enriched uranium, which is used in the construction of a nuclear weapon, has such a long half-life that it emits too little radiation to be readily detected as well.

This leaves as the final safeguard the radiation portals put in place by CBP at the exit of gates of U.S. ports or at our border crossings with Canada and Mexico. Outside of the fact that a container that might contain a dirty bomb can expect to spend a day or more within the terminal before passing by this detection equipment, thereby placing the port facility itself at risk in the interim, the radiation portals used by CBP suffers from the same limitation as those operating overseas under DOE's auspices.

In the end, the container security measures being pursued by the U.S. government resembles a house of cards. In all likelihood, when the next terrorist attack occurs on U.S. soil and it involves a maritime container it will have come in contact with most or even all the these new security protocols. That is, the container likely will be from a C-TPAT company. It will have originated or been transshipped through a CSI port. It will have been handled in an ISPS compliant marine facility and crossed the ocean on an ISPS complaint ship. It will have passed through a radiation portal and gone undetected. As a consequence, when the attack happens, the entire security regime will implicated generating tremendous political pressure to abandon it.

.

We can do better. With relatively modest investments and a bit of ingenuity, the international intermodal system and global supply chains can have credible security while simultaneously improving their efficiency and reliability. What is required are a series of measures that collectively enhance visibility and accountability within global supply chains.

As a starting point, the United States should work with the Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in authorizing third parties to conduct validation audits of the security protocols contained in the International Ship and Port Facility Security Code and the World Customs Organization's new framework for security and trade facilitation. The companies carrying out these inspections should be required to post a bond as a guarantor against substandard performance and be provided with appropriate liability protections should good-faith efforts prove insufficient to prevent a security breech. A multilateral auditing organization made up of experienced inspectors and modeled on the International Atomic Energy Commission should be created to periodically audit the third party auditors. This organization also should be charged with investigating major incidents and when appropriate, recommend changes to established security protocols.

To minimize the risk that containers will be targeted by terrorist organizations between the factory and a loading port, the next step must be for governments to create incentives for the speedy adoption of technical standards developed by the International Standards Organization for tracking a container and monitoring its integrity. The Radio Frequency Identification (RFID) technologies now being used by the U.S. Department of Defense for the global movement of military goods can provide a model for such a regime.

Washington should next embrace and actively promote the widespread adoption of a novel container security project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong. Mr. Chairman, I know that you have seen this pilot in operation this past December, and just this weekend, two of your colleagues, Senator Lindsey Graham and Senator Charles Schumer have done so as well. On April 1, 2006, DHS Secretary Michael Chertoff will be visiting Hong Kong to examine the pilot as well.

As you know, starting in late 2004, every container arriving in the two main truck gates of two of the busiest marine terminals in the world are, at average speeds of 15 kph, have been passing through a gamma ray machine to scan its contents, a radiation portal to record the levels of radioactivity found within the container, and optical character recognition cameras which photograph the number painted on the top, back, and two sides of the container. These scanned images, radiation profiles, and digital photos are then being stored in a database for customs authorities to immediately access if and when they want.

The marine terminals in Hong Kong led by Group Managing Director John Meredith of Hutchison Port Holdings and Managing Director Sean Kelly of Modern Terminals have invested in this system for three reasons. Most importantly, they are hoping that this 100 percent scanning regime will deter a terrorist organization from placing a weapon of mass destruction in a container passing through their port facilities. Because the contents of every container are being scanned, should a terrorist organization try to shield a radioactive bomb or fissile material to defeat the radiation portals, it will be relatively easy to detect the shielding material because of its density. A second reason for making this investment is to minimize the potential disruption associated with targeting containers for an inspection at the loading port. The system will allow the container to receive a preliminary inspection remotely without the container having to be removed from the marine terminal, transported to an inspection facility operated by Hong Kong customs authorities, and after the inspection, returned to the terminal but likely too late to be loaded on the ship for its scheduled voyage. The third reason is that by maintaining a record of the contents of every container entering their terminal, the port is able to provide government authorities with a forensic tool that can support a follow-up investigation should a container still slip through with a weapon of mass destruction. This tool would allow authorities to quickly isolate to a single supply chain where the security compromise took place, thereby minimizing the risk that a port-wide shut down will be necessary. In other words, by scanning every container, the marine terminals in Hong Kong are well positioned to indemnify the port for security breeches that occur upstream. As result, a terrorist would be unable to successfully generate enough fear and uncertainty to warrant shutting down one of the most important transportation hubs of the global trade system.

This low-cost system of inspection is being carried out without impeding the operations of these very busy marine terminals. It could be put in place in every major container port in the world at an estimated cost of $1.5 billion or approximately $10-25 per container, depending on the volume of containers moving through the terminal. The system could be paid for by authorizing ports to collect user fees that cover the costs associated with purchasing the equipment, maintaining its upkeep, and investing in upgrades when appropriate. Once such a system is operating globally, each nation would be in a position to monitor its exports and to spot-check their imports against the images first collected at the loading port.

From the standpoint of U.S. security, the biggest value of this system should it be widely deployed are twofold. First, it provides a powerful deterrent to discourage terrorists from *exploiting* global supply chains as a conduit for a weapon of mass destruction. This importantly also includes its counterproliferation potential. If such a system were in place in the terminals owned and operated by Hutchison Port Holdings and Dubai Port World in the port of Karachi Pakistan, it would make that port a far less attractive place through which to smuggle nuclear materials to the Middle East. The same holds true of ports along coastal China near North Korea. Second, it creates a powerful deterrent to discourage terrorists from *targeting* the global supply chains with a “dirty bomb” since the inspection system will make the intermodal system far more resilient in managing a breach of security without a wholesale shutdown of the trade system.

The total cost of third party compliance inspections, deploying “smart” containers, and operating a cargo scanning system such as the one being piloted in Hong Kong likely reach $50 to $100 per container depending on the number of containers an importer has and the complexity of its supply chain. Such an investment would allow container security to quickly move from the current “trust, but don’t verify” system to a “trust but verify” one. Can industry afford the cost of this regime? Even if the final price tag came in at $100 additional cost per container, it would raise the average price of cargo moved by Wal-Mart or Target by only .2 percent. What importers and consumers are getting in return for that investment is both the reduced risk of a catastrophic terrorist attack and the cascading economic consequences flowing from such an attack.

Happily, developing the means to track and verify the status of containers provides benefits that go beyond security. This is because there is a powerful commercial case for constructing this capability as well. When retailers and manufacturers can monitor the status of all their orders, they can confidently reach out to a wider array of suppliers to provide them what they need at the best price. They also can trim their overhead costs by reducing inventories with less risk that they will be left short.

Transportation providers will benefit from greater visibility as well. Terminal operators and container ships, that have earlier and more detailed information about incoming goods, can develop load plans for outbound vessels in advance and direct truck movements with greater efficiency.

Greater visibility also brings potential benefits for dealing with insurance issues. Knowing precisely where and when a theft takes place makes it easier to decipher the nature of the threat and to identify what breaches, if any, contributed to the loss. When there is damage, it is much easier to track down the responsible parties. In short, rather than spreading the risk across the entire transportation community, insurance premiums can be more carefully tailored. In turn, that creates a stronger market incentive for all the participants in the supply chain to exercise greater care.

Even if there were no terrorist threat, there are ample reasons for individual governments, ASEAN, the European Union, WTO, and other regional and international organizations to place port, border, and transportation security at the top of the multilateral agenda. Enhance controls within the global trade lanes will help all countries reduce theft; stop the smuggling of drugs, humans, and counterfeit goods; crack down on tariff evasion; and improve export controls.

At the end of the day, confronting the nuclear smuggling threat requires that we take the post-9/11 security framework the U.S. government has been developing largely on the fly over the past four years, and quickly move it to the next generation of initiatives that build on the original framework. We have a version 1.0. We need a version 2.0. The three key ingredients of getting from where we are to where we must be are: (1) to recognize that it is a global network that we are trying to secure; (2) that much of that network is owned and operated by private entities, many who have foreign ownership so U.S. government must be willing and able to work with those companies as well as their host governments so as to advance appropriate safeguards, and (3) both Congress and the White House should embrace a framework of "trust but verify," in President Ronald Reagan's phrase, based on real global standards and meaningful international oversight.

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

Stephen Flynn is the author of *America the Vulnerable*. He is currently writing a new book to be published by Random House in Fall 2006 entitled, *The Edge of Disaster: Catastrophic Storms, Terror, and American Recklessness*. He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report "*America: Still Unprepared—Still in Danger,*" co-chaired by former Senators Gary Hart and Warren Rudman. Since 9/11 he has provided congressional testimony on homeland security matters on fifteen occasions. He spent twenty years as a commissioned officer in the U.S. Coast Guard including 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.