COUNCIL ON FOREIGN RELATIONS

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

"Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative"

Written Testimony before

a hearing of the

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

on

"The Container Security Initiative and the Customs-Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?"

by

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

Room 562
Dirksen Senate Office Building
Washington, D.C.

9:30 a.m.
May 26, 2005

"Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI)"

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 this morning to discuss two of the Department of Homeland Security's cornerstone programs to advance container security. The stakes associated with preventing containers from being exploited as a poor man's missile are enormous. Should a terrorist organization successfully smuggle a weapon of mass destruction into the United States and detonate it on our nation's soil, untold American lives would be in jeopardy. But such an attack also would almost certainly lead U.S. officials to close U.S. ports and borders to all inbound containers until they could assess the likelihood of follow-on attacks. If that closure extended to two or three weeks it would bring the global intermodal transportation system to its knees. Since two thirds of the total value of U.S. maritime overseas trade move in containers, American manufacturers that rely upon those shipments to keep their assembly plants operating and retailers who depend upon them to keep their shelves stocked would quickly become a part of the collateral damage. All together, the cascading costs of a weeks-long shutdown in the aftermath of a WMD attack would almost certainly be in the hundreds of billions of dollars.

As I will outline below, the Government Accountability Office is largely on the mark in highlighting a number of serious shortcomings of the C-TPAT and CSI programs as they are currently operating. However, as a stepping-off point, I believe that it is appropriate to recognize and applaud the leadership of Commissioner Robert Bonner in crafting and quickly deploying these initiatives to redress what has been a longstanding vulnerability to America's security. The objectives of these programs represent both a dramatic and constructive change in the way nations and companies have approached the issue of trade and transportation security. Among the highlights are:

- C-TPAT has helped to usher in a fundamental change in how most companies and customs officials view their respective roles in container security.

Prior to 9/11, the relationship between customs authorities and importers and exporters was marked by both sides approaching one another with an "us-versus-them" mentality. Customs officials saw themselves engaged in the often thankless job of trying to enforce trade laws, collect revenues, and detect and intercept contraband in the face of an ambivalent and at times, antagonistic private sector. Companies were focused on optimizing their ability to move in and out of the U.S. market at the lowest possible cost with the least amount of risk of delay. Customs regulations and enforcement activities were widely perceived as barriers to that objective. Should customs inspectors discover an infraction, the typical industry response was to treat the occasional fine as the cost of doing business. Only on rare occasions would companies make the effort to change their

operations to improve their ability to comply with the rules. C-TPAT has helped to transform this "cat-and-mouse" relationship by generating a wider appreciation within the private sector that importers and exporters must be a constructive partner in bolstering supply chain security.

- CSI creates an important opportunity for detecting and intercepting potentially dangerous cargoes before they are loaded on an ocean carrier destined for a U.S. port.

Every major U.S. container port contains other critical infrastructures such as energy refineries, chemical facilities, and power plants. And all of them are close to large urban population centers. This makes the risk associated with discovering a WMD once it is inside a U.S. port (where it could potentially be remotely detonated) unacceptably high. In addition, once a container is loaded aboard a container vessel, it is almost impossible to gain access to it. Upwards of 17 containers can be stacked on top of one another on modern container ships. The space between one stack of containers and another is often as little as eight inches. This makes it practically impossible to verify that a WMD is in a container once it is at sea. Should one be detected, the vessel would have to be diverted to a remote location where the container could be unloaded. In the interim the thousands of other containers onboard that vessel would be delayed. The best way to deal with these practical challenges is to check containers before they are loaded on a U.S.-bound ocean carrier. CSI provides a way to accomplish this.

- CSI has the potential to promote greater levels of cooperation and accountability among customs agencies.

One of the greatest benefits of deploying customs agents overseas is the potential for fostering greater levels of international cooperation, promoting professionalism, and improving information sharing among customs agents. In addition, CSI helps to reverse a trend over the past few decades towards nations making only a cursory effort to monitor the exports leaving their jurisdictions. The downside of replying primarily on import inspections to enforce rules is that it makes it much harder to assign accountability when infractions are discovered. However, the emphasis on identifying and inspecting suspicious shipments before they are loaded helps to isolate the source of illicit activity and puts the host government on notice should the problem originate within their jurisdiction.

While in principle, C-TPAT and CSI provide an excellent foundation for bolstering container security, the current way these programs are being resourced and managed is largely undercutting that potential. Among the major problems are the following:

1. The voluntary nature of C-TPAT and CSI translates into it being a "trust, but don't verify" system. The benefit of facilitated access to the U.S. market is offered without validating in advance that the participants are taking sufficient measures to ensure that they will not be compromised. This is because CBP lacks the resources and the jurisdictional reach to confirm that the thousands of C-TPAT participants are carrying out the security measures contained in their application profile. Approval is provided on the

basis of having no prior negative compliance violations and the absence of information from intelligence databases that would cause concern. In short, past performance is presumed to be a predictor of future results. There is no requirement that companies update their plans at established intervals or resubmit their plans should they make changes to their supply chains. The process of validation is essentially a "spot-check" whereby CBP inspectors first notify the participant of a pending inspection and then enter into a joint negotiation of what will be covered. Even this restrictive protocol has been barely implemented because CBP has not yet been provided adequate resources to hire and train the staff to carry out the validation process for all the current C-TPAT participants and those with outstanding applications.

CSI currently suffers from a similar problem of providing membership without requiring that the host country demonstrate their ability to conduct inspections based on an established set of criteria. For instance, there are no performance-based criteria such as the existence of a training and evaluation program for inspectors, adequate maintenance of non-intrusive inspection equipment, and periodic exercises to test the capacity of the host country to detect and respond when the system alarms on suspicious material.

2. As it currently operates, C-TPAT inadvertently may be actually raising the risk of a WMD being smuggled into the United States via a participant's supply chain. This is because CBP is placing too much reliance on the capacity of legitimate companies to independently put in place adequate supply chain security measures to deter terrorist groups from exploiting those chains. At the same time, it is has excessive faith in the intelligence it is able to collect or gain access to. Finally, it's "risk-managed" approach is premised on the flawed assumption that terrorists are most likely to target companies that: (a) have been historically susceptible to organized crime and smugglers, (b) have demonstrated a weak record of customs compliance, or (c) are new commercial entities. CBP approach is summed-up by Commissioner Bonner as: "We are inspecting 100 percent of the 'right' 5-6 percent of containers that pose the greatest threat."

Unfortunately, private companies are unlikely to have in place adequate safeguards to deter a determined terrorist, armed with a WMD. This is because private security is inherently reactive; i.e., companies cannot punish violators of their rules until there is some evidence that those rules have been broken. A good chief security officer puts in place measures that allow them to detect aberrant activity once it occurs. They then conduct professional investigations to confirm any infractions of company rules or possible crimes. The results of their investigations are passed along to senior managers who impose meaningful sanctions or refer the incident to law enforcement authorities when appropriate. When these sanctions are applied, other employees who might be tempted to disobey the rules become aware of the risk of being caught, so they are deterred.

In the case of smuggling or customs fraud, traditional corporate security is generally up to the task of deterring criminals. This is because smuggling and cheating typically involve ongoing conspiracies. Few criminals have the discipline to cheat, steal, or smuggle just once. Inevitably, if they succeed the first time, they try again and again.

Since these repeat violations can be spotted and sanctioned by legitimate companies, criminals have to gravitate to the environments where the controls are weakest.

But the approach a smuggler takes to smuggling a WMD into the United States is likely to be different. First, terrorists may have to spend years acquiring 1-2 weapons. Once they have them, they are likely to be more than content to be successful on their first and only attempt. Since they know legitimate companies are viewed with much less scrutiny by U.S. authorities, it is these companies that present the best opportunity to get into the United State undetected if they can identify and exploit a vulnerability. Since no company has a fail-safe security system, they can be confident that they can locate and successfully compromise an existing safeguard at least once. It may be as simple as offering a large bribe to a truck driver to take an extended lunch break so that operatives can gain access to his load. A driver who repeatedly takes long lunch breaks might be noticed by a company with tight security controls. But only under extraordinary circumstances would a company have a system in place to detect such an infraction in real time the first time it takes place, particularly if the incident happens in overseas location between the factory where the container is stuffed and the loading port where it is being shipped to the United States. The only hope CBP has of detecting such a scenario is to have routine access to reliable intelligence about the identities and activities of terrorists. But this is a very weak reed to rely upon given the current difficulties the U.S. intelligence community is facing in adapting to the counter-terrorism mission.

The second reason for a terrorist organization to explicitly target a C-TPAT participant is that a successful penetration will have the derivative advantage of eroding public trust in the U.S. government's risk-management model. If a terrorist group can succeed at carrying out a WMD attack with what CBP has declared to be a "low-risk" container, all containers thereafter will be viewed as "high-risk." This will inevitably generate irresistible political pressure to subject all containers to a comprehensive inspection. The resultant widespread economic and societal disruption and billions of dollars of costs which would arise from a post-attack "100 percent" inspection regime would have real military value for our enemies.

3. The lack of specific standards under C-TPAT that are uniformly enforced is undermining the incentive for legitimate companies to invest in upgraded supply chain security measures. Security is not free. A C-TPAT participant incurs costs when it invests in measures to bolster its security protocols. Given the sheer numbers of companies participating in the program and the well-advertised lack of CBP's capacity to validate compliance, companies that are sincerely committed to improving their security have to worry about the likelihood that it has competitors who end up being free riders. In other words, they have to be mindful of potentially putting themselves at a competitive disadvantage by investing in security while others are doing little to nothing but receiving the same benefits from CBP. Absent a sense that there is a level playing field, executives become understandably reluctant to do more than the bare minimum to comply.

4. To the extent that resource constraints prevent CBP from extending CSI to less developed countries, we may end up indirectly creating a barrier to trade with those

nations. This then has the unintended consequence of eroding the development prospects for those countries, thereby creating the very conditions that fuel the terrorist threat.

5. There are conflicts between the operation of CSI and C-TPAT and the International Ship and Port Facility Security Code (ISPS) that came into effect on 1 July 2004. ISPS establishes minimum international security requirements for all ocean carriers and marine terminals, but does not address the cargo security issue. C-TPAT places requirements which are redundant or exceed the ISPS mandates on ocean carriers and marine terminals but participation is voluntary. CSI places some poorly defined requirements on the ports who are participating, but it is not a universal program. Consequently, should there be intelligence of a pending attack or an actual attack that results in maritime authorities elevating the ISPS three-tiered alert level, CBP's promised benefit of greater facilitation will be compromised. This is because a ship will almost always be carrying containers that are mixture of C-TPAT and non-C-TPAT participants and which originate from both CSI and non-CSI ports. Therefore, as a practical matter, under the rules governing the ISPS code, the ship and the receiving terminal will be subjected to the same heightened security requirements and the associated delays regardless of whether or not the cargo is from a C-TPAT company and a CSI port.

The shortcomings I have outlined above are very serious, but they all can be addressed at a reasonable cost, making it possible to advance the very positive objectives that spawned CSI and C-TPAT in the first place.

1. The way to advance the credibility of C-TPAT is for DHS to authorize third parties to conduct the validation audits of the proposed security protocols. DHS can require that these companies post a bond as a guarantor against substandard performance. These third parties will need to be given some liability protection by the federal government should their good-faith efforts fail. DHS must also have the means to "audit the auditors" to maintain high standards.

There are models for this. In the maritime area, the Coast Guard has long authorized "professional classification societies" to conduct inspections to determine if a ship is compliant with international shipping safety standards. These third party organizations are able to maintain the requisite technical expertise at a higher level than is possible within the federal government. They are also able to operate in overseas jurisdictions where U.S. officials may not be welcome. To keep the system honest, the Coast Guard periodically inspects vessels entering U.S. waters. Should it find that the vessel is in violation of the international standards, it will not only hold up that ship until corrective actions are taken, but it will target for inspection all other vessels who have been certified by the same classification society.

2. To minimize the risk that containers from C-TPAT participants will be targeted by terrorist organizations between the factory and the loading port, the U.S. government needs to work with the European Union and its other allies in advancing a standard for tracking a container and monitoring its integrity. The Radio Frequency Identification (RFID) technologies now being used by the Department of Defense for the global

movement of military goods can provide the foundation for putting in place such a regime.

3. The U.S. government should endorse a pilot project being sponsored by the Container Terminal Operators Association (CTOA) of Hong Kong in which every container arriving in the two of the busiest marine terminals in the world are, at average speeds of 15 kph, passing through gamma ray machine, a radiation portal, and optical character recognition cameras which record the container number. These images and radiation profiles are then being stored in a database allowing the virtual inspection of any and all containers entering the terminal. The cost of deploying and maintaining this system throughout the entire port it estimated to be $6.50 per container.

The port of Hong Kong has 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 WMD in a container passing through their port. Second, should a container be targeted under the CSI agreement between CBP and Hong Kong Customs & Excise, the system will allow the box to be inspected without the importer having to pay for the "service" of having the container removed from the marine terminal, transported to a Customs & Excise inspection facility, and returned by which time it would almost certainly miss its scheduled voyage. Last, 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 WMD. Their incentive to do so is that if an incident can be quickly isolated to a single supply chain then there will be no need for a port-wide shut down. In other words, by scanning every container, they are well positioned to indemnify the port as the source of a potential security breech. As result, a terrorist would be deprived of the collateral consequence of mass disruption of the intermodal transportation system.

This low-cost system of inspection is being carried out with no adverse impact on the marine terminals operations and without any U.S. government funding. It could be put in place globally at a cost of $1.5 billion or roughly $10 per container. Along with the third party inspection of C-TPAT compliance, establishing standards that support the deployment of "smart" containers at an estimated cost of $50 per shipment, we can move from the current "trust, but don't verify" system to a "trust but verify" one. Can industry afford the cost of this regime? To put the figures into context, the average container moved by Target or Wal-Mart from Asia to the United States carries approximately $60,000 in merchandise. Even a total of $100 additional cost per container would raise the price of those goods by .06 percent. What consumers are getting in return for that investment is both the reduced risk of a WMD attack and the cascading economic consequences flowing from such an attack which could hold the potential of generating a global recession. In short, this is about the soundest investment that they could make towards buying an added measure of security in our post-9/11 world.

4. The U.S. Department of State should lead a federal effort to have international development organizations; e.g., the World Bank, regional banks, WTO, etc., provide the

less develop countries with the non-intrusive inspection equipment, training, and data management tools to examine cargo entering and leaving their jurisdictions.

5. CSI and C-TPAT should be linked to the ISPS code.

When Commissioner Bonner first announced what has become the Container Security Initiative in a speech at CSIS in January 2002 he said:

> *As with any new proposal, implementation of this initiative will not be easy. But the size and scope of the task pale in comparison with what is at stake. And that is nothing less than the integrity of our global trading system upon which the world economy depends.*

These words are as true today as they were just four months after 9/11. What is required as we move forward is a willingness to both critically evaluate where we are and to make mid-course adjustments that keep us steaming rapidly ahead. That is why the oversight work of this committee and this hearing today is so important.

The biggest barrier to progress right now is the reluctance by DHS to make several necessary mid-course changes:

CBP has been resistant to the idea of 3rd party inspectors for C-TPAT compliance even though: (a) they are hopelessly behind in processing applications, (b) they have only a few inspectors who currently have adequate experience and training in supply chain security, and (c) they lack the legal authority to carry out validation inspections overseas.

While CBP has been generally supportive of deploying electronic container seals, they have shown little interest in technologies that could monitor the location of containers as they move through the transportation system. They also have not yet communicated to the port of Hong Kong an indication of their interest or support for the cargo container inspection project now underway there.

My experience interacting with CBP on these initiatives over the past 3 ½ years is that their ambivalence about embracing new technologies that are deployed to confirm that low risk participants in the trade system are indeed low risk stems from four sources. First, they are reluctant to acknowledge that many of their pre-9/11 risk management assumptions may not be well-suited for the low-probability but high consequence threat posed by the WMD in a container. Second, they are reluctant to "deputize" to the private sector functions historically performed by customs agents. Third, beyond the requirement that ocean carriers provide them with cargo manifests, they have traditionally maintained nominal interactions with the transportation industry, focusing instead on importers and exporters and trade intermediaries. Last, they are queasy about being given more data than they are in a position to examine and analyze. This creates a collateral bureaucratic risk of being held accountable should a post-mortem investigation reveal that they had data in their possession, but failed to look closely at it.

But my experience has also been that CBP is populated with dedicated and hardworking professionals who take their jobs extremely seriously. They work with far fewer resources than they deserve and receive too little credit for the important job they perform each day. C-TPAT and CSI demonstrates their ability to be both innovative and adaptive in the face of a new threat. These programs deserve the support of the administration, the Congress, and the American people. But, much work remains to be done towards ensuring they are a match for the catastrophic terrorist threat we face in the 21st century.