REPORTS FOLLOW
TABLE OF CONTENTS
AND EXHIBIT LIST.
Report on page 503.

S. Hrg. 109–548

NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN

HEARINGS

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 28 AND 30, 2006

Printed for the use of the Committee on Homeland Security
and Governmental Affairs

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Chief Counsel*
TRINA D. TYRER, *Chief Clerk*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

NORM COLEMAN, Minnesota, *Chairman*

TED STEVENS, Alaska
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

RAYMOND V. SHEPHERD, III, *Staff Director and Chief Counsel*
BRIAN M. WHITE, *Professional Staff Member*
ELISE J. BEAN, *Minority Staff Director and Chief Counsel*
LAURA E. STUBER, *Minority Counsel*
MARY D. ROBERTSON, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, MARCH 28, 2006

THURSDAY, MARCH 30, 2006

ALPHABETICAL LIST OF WITNESSES

EXHIBITS

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Norm Coleman, Chairman
Carl Levin, Ranking Minority Member

AN ASSESSMENT OF U.S. EFFORTS TO SECURE THE GLOBAL SUPPLY CHAIN

PREPARED BY THE

MAJORITY AND MINORITY STAFF
OF THE
PERMANENT SUBCOMMITTEE
ON INVESTIGATIONS

RELEASED IN CONJUNCTION WITH THE
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
MARCH 30, 2006 HEARING

NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT:
SECURING THE GLOBAL SUPPLY CHAIN

I. INTRODUCTION

Since early 2003, the United States Senate Permanent Subcommittee on Investigations (PSI or the Subcommittee) has conducted an oversight investigation into U.S. Government programs designed to secure the global supply chain. This effort has been thoroughly bipartisan and bicameral. The Subcommittee's efforts have included: document requests and letters from the Subcommittee,[1] numerous meetings with officials from the U.S. Departments of Homeland Security (DHS) and Energy (DOE), staff assessments of ten Container Security Initiative ports,[2] staff examinations of eight U.S. ports of entry,[3] a staff trip to the Nevada detection equipment test site, and a staff inspection of the National Targeting Center (NTC). Subcommittee staff has also met with officials from Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), the Domestic Nuclear Detection Office (DNDO), and the National Nuclear Security Administration (NNSA). This report details the findings from the Subcommittee's investigation, outlines areas of concern, and makes recommendations for improving and enhancing the security of the global supply chain.

The support and leadership of Homeland Security and Governmental Affairs Committee Chairman Susan Collins and Ranking Member Joseph Lieberman has been crucial to PSI's investigation. In addition, Congressman John Dingell, the Ranking Member of the U.S. House of Representatives Energy and Commerce Committee, actively participated in this oversight investigation.[4]

II. EXECUTIVE SUMMARY

This report provides an unvarnished assessment of the state of global supply chain security. The Subcommittee staff's findings are troubling. In short, America's supply chain security remains vulnerable to the proverbial Trojan Horse – America's enemies could compromise the global supply chain to smuggle a Weapon of Mass Destruction (WMD), or even terrorists, into this country.[5]

These frightening scenarios are not the work of Hollywood writers. Last year, on two separate occasions, dozens of Chinese immigrants were smuggled through the Port of Hong Kong into Los Angeles using maritime shipping containers. These incidents, coupled with similar episodes abroad, demonstrate the vulnerability of the global supply chain. The 9/11 Commission confirmed these vulnerabilities, stating: "opportunities to do harm are as great, or greater, in maritime or surface transportation."[6]

Over the course of its three-year investigation, Subcommittee staff has identified numerous weaknesses in America's programs that secure the global supply chain. A brief overview of these problems illustrates the challenges confronting these efforts:

- In the Container Security Initiative (CSI), a critical program designed to inspect high-risk shipping containers before they enter U.S. ports, the Subcommittee found that only a *de minimus* number of such high-risk containers are actually inspected. In fact, the vast majority of high-risk containers are simply not inspected overseas. To make matters worse, the U.S. Government has not established minimum standards for these inspections.

---

[1] *See* Appendix A.

[2] *See* Appendix C.

[3] *See* Appendix D.

[4] PSI staff would also be remiss if they did not acknowledge the insights and efforts of U.S Senate Homeland Security and Governmental Affairs Committee Staffers Kathleen Kraninger and Jason Yanussi, U.S. House of Representatives Energy and Commerce Committee Staffer Chris Knauer, and U.S. House of Representatives Homeland Security Staffers Al Thompson and Michael Geffroy.

[5] The term "WMD" refers to a biological, chemical, radiological, or nuclear weapon utilized in such a manner to harm or kill large numbers of people.

[6] *See* Final Report of the National Commission on Terrorist Attacks Upon the United States, p. 391.

- Under the Customs-Trade Partnership Against Terrorism (C-TPAT), the U.S. Government grants benefits to private-sector companies that make specific security commitments. The Subcommittee found, however, that an overwhelming proportion of participating companies receive benefits prior to having their security profile validated. Only 27 percent of the participating companies have been subjected to a validation. Therefore, 73 percent of companies have not been subjected to any legitimate, on-site review to ensure that their security practices pass muster.[7]

- The targeting system employed by the U.S. Government to identify high-risk shipping containers entering U.S. ports is largely dependent on "the least reliable" form of data for targeting purposes.[8] Moreover, the Subcommittee has found that this targeting system has never been tested or validated, and may not discern actual, realistic risks.

- Less than 40 percent of cargo containers entering U.S. ports are screened for nuclear or radiological materials. One part of the problem is that the deployment of radiation detection equipment is woefully behind schedule. As of March 2006, the Department of Homeland Security has deployed only 30.8 percent of the necessary radiation monitors. [9]

Although these findings are alarming, there are some silver linings. For instance, the creation of the Domestic Nuclear Detection Office (DNDO) has already addressed some of the problems surrounding the deployment of radiation detectors. DNDO has created a centralized, global architecture for the deployment of these radiation detectors, so that the process is no longer diffused among several disconnected agencies. DNDO has begun to address the concerns of numerous private-sector port operators, which had reservations about the safety and impact of radiation monitors upon their operations. DNDO has also facilitated the installation of numerous radiation detectors.

The good news is not limited to DNDO. While the United States currently screens approximately 5 percent of all maritime containers,[10] there is a promising pilot project in the Port of Hong Kong that demonstrates the potential to screen 100 percent of all shipping containers.[11] Each container in the Hong Kong port flows through an integrated system featuring an imaging machine, a radiation scan, and a system to identify the container.[12] Coupling these technologies together allows for the most complete scan of a container currently available. The Hong Kong concept or similar technology, which is described in detail in this report, holds great promise and could lead to a dramatic improvement in the efficacy of our supply chain security. These improvements would help ensure that the threat of Trojan Horse infiltration by terrorists never becomes a reality.

III. THE CHALLENGE AND THREAT

Maritime trade is one of the foundations of our global economy. Seaports are critical gateways for international trade, and shipping containers play a vital role in the movement of cargo between global trading partners. Approximately 90 percent of the world's trade is shipped in containers. Effectively securing cargo and ensuring the viability of the global supply chain is critical to homeland security and the global economy.

The standardization of containers changed a rather laborious shipping process into an efficient global system. Today, containers serve as portable warehouses for almost every type of cargo and containers are configured with refrigeration technology for frozen goods or hanger systems for garments. Maritime commerce, and container shipping in particular, provides a

---

[7] Subcommittee staff meeting with CBP on March 20, 2006.

[8] *See* GAO Report-04-352NI, "Homeland Security Challenges Remain in the Targeting of Oceangoing Cargo Containers for Inspection," February 2004, p. 26.

[9] This data was supplied to the Subcommittee by CBP in March 2006.

[10] This number refers to either a non-intrusive exam or a physical inspection.

[11] This number refers to a non-intrusive and radiation exam.

[12] *See* further discussion of this concept in Section G. It is important to note that Subcommittee staff is not endorsing this product, rather the concept that has been demonstrated in Hong Kong.

highly attractive means of delivering commerce across the world. Unfortunately, the characteristics that make containers attractive for delivering goods also make them attractive for delivery of weapons, including nuclear and radiological devices.

The abundant cargo space of the international standard 8-foot by 8-foot container, which ranges in length from 20 to 48 feet, affords a perfect vehicle to convey weapons. Such containers may house large devices, so that the container itself may be part of the weapon, as well as small, concealed devices, intended for receipt and use by an agent in the destination country. Thus, nuclear, radiological, and large conventional weaponry could be shipped, as well as chemical, biological, or small conventional devices. For example, unaccounted-for, anti-aircraft Stinger missiles remaining from the Afghan-Soviet war could be smuggled into the United States via a maritime container.

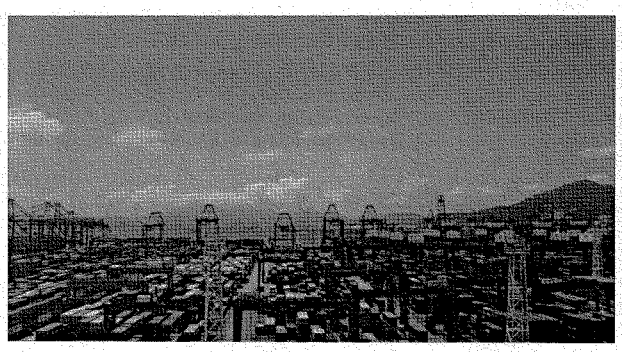


Figure 1. As the world's busiest port, Hong Kong illustrates the challenges of securing the global supply chain.

Containers may also serve as ideal platforms to transport potential terrorists into the United States. Less than a month after the September 11th attacks, an incident in Gioia Tauro, Italy highlighted the vulnerabilities in the global supply chain. In October 2001, port authority officials heard strange noises from a 40-foot shipping container. Inside the container, officials found a well-dressed, Egyptian-born Canadian by the name of Amir Farid Rizk. The container had been outfitted with a bed and a makeshift toilet. Mr. Rizk was alone in the container, but was equipped with a satellite phone, a laptop, false credit cards and security passes for airports in Egypt, Thailand, and Canada. Mr. Rizk was charged with terrorism but later released when his lawyers argued that he was fleeing religious and legal persecution in Egypt.[13] The discovery of Mr. Rizk underscored the vulnerabilities of the global supply chain.

Two incidents at the Port of Los Angeles/Long Beach (LA/LB) last year demonstrated that terrorists could be smuggled into the U.S. in a container. On January 15, 2005, 32 Chinese immigrants were arrested as they emerged from a container on board a ship at the Port of Los Angeles. The immigrants had been apparently placed inside the container at Shekou, China, and were then shipped through the Container Security Initiative (CSI) Port of Hong Kong. The container was shipped aboard a carrier owned and operated by a Customs-Trade Partnership Against Terrorism (C-TPAT) certified member. Fourteen days later, the immigrants were unloaded from that container at the Port of Los Angeles.[14] A similar, almost identical, incident took place on April 2, 2005, in which 29 Chinese immigrants were found emerging from a maritime container that had just arrived in Los Angeles. Once again, the Chinese immigrants had been loaded into a container in Shekou and the ship had moved through the CSI Port of Hong Kong and proceeded on to Los Angeles.[15]

---

[13] The Institute for Counter-Terrorism, "Suicide bombing at Ashdod Port," March 14, 2004, *http://www.ict.org.il/spotlight/det.cfm?id=972*, accessed March 14, 2006.

[14] Eric Slater, "Human Smuggling Operation Probed," *Los Angeles Times*, January 17, 2005.

[15] Greg Krikorian, "Chinese Smuggled into Port Arrested," *Los Angeles Times*, April 5, 2005.

The disturbing lessons of these incidents are clear: the same maneuver could be used to smuggle members of terrorist organizations or a WMD into the United States. According to Director of National Intelligence John Negroponte, "Attacking the U.S. Homeland, US interests overseas, and US allies – in that order – are al-Qa'ida's top operational priorities .... Although an attack using conventional explosives continues to be the most *probable* scenario, al-Qa'ida remains interested in acquiring chemical, biological, radiological, and nuclear materials or weapons to attack the United States, U.S. troops, and U.S. interests worldwide."[16] Clearly, the threat is real and, given the importance of trade to our nation's economy, it is critical that we secure the global supply chain.

SUICIDE BOMBERS HIDDEN IN CONTAINER

An incident at the Port of Ashdod in Israel demonstrated the use of shipping containers to hide dangerous terrorists. In March of 2004, two Palestinian suicide bombers hid in a shipping container that had been brought from Gaza on board a truck and were thus able to enter the port. The two suicide bombers killed ten people and wounded 16 others. It is suspected that the suicide bombers were intending to blow themselves up near the tanks of hazardous chemicals. A search of the shipping container revealed five unexploded grenades and the remains of several meals in a hidden compartment in the suspect container. *See* The Institute for Counter-Terrorism, "Suicide bombing at Ashdod Port," March 14, 2004, http://www.ict.org.il/spotlight/det.cfm?id=972, accessed March 14, 2006.

A. The Global Supply Chain

The multitude of parties and transactions involved in the typical container shipping process makes it difficult to ensure the integrity of container cargo. The parties involved in a typical shipment include the exporter, importer, freight forwarder, customs broker, customs inspector, inland transportation provider(s) (which may include more than one trucker or railroad), port operators, possibly a feeder ship, and ultimately an ocean carrier. Compounding the number of parties and transactions involved, container ships usually carry cargo from hundreds of different companies, and a single container often carries cargo for several different customers. As a result, a single consolidated container shipment may generate 30 to 40 sets of documents and bills of lading.[17]

Each transfer of a container in this complex and tiered shipping process constitutes a point of vulnerability in the supply chain. Increasing these supply chain vulnerabilities, individual shipping containers are typically loaded at a number of different company warehouses, and not at the ports of departure. Therefore, ensuring that containers that eventually enter the United States are not "stuffed" with illegitimate cargo at overseas factories or consolidation centers, or at any other point in transit to the United States, is a critical challenge facing our supply chain security.

Since inspecting cargo on the high seas is practically impossible and inspecting cargo upon its arrival at a U.S. port may come too late to prevent a terrorist event, it is imperative that cargo is evaluated and secured at its point of origin. The best way to accomplish this is to ensure that the cargo information for every container that enters the United States is fully and accurately reported to CBP. Therefore, confirmation of the security of each transfer facility and the trustworthiness of every company involved in the multi-tiered shipping process is absolutely critical.

IV. U.S. GOVERNMENT EFFORTS TO SECURE THE GLOBAL SUPPLY CHAIN

A. Overview of Initiatives

The primary federal government programs to secure the global supply chain are:

- The Container Security Initiative (CSI);
- The Customs-Trade Partnership Against Terrorism (C-TPAT);
- The Megaports Initiative; and
- The Radiation Portal Monitor Project (RPMP).

---

[16] *See* Statement of John D. Negroponte, "Annual Threat Assessment of the Director of National Intelligence," before the Senate Select Committee on Intelligence, February 2, 2006.

[17] The term "bill of lading" refers to a document issued by a carrier to a shipper listing and acknowledging receipt of goods for transport, and specifying the terms of delivery.

In early 2002, following the attacks of September 11th, the U.S. Customs Service launched both the Container Security Initiative and the Customs-Trade Partnership Against Terrorism to address the threat of terrorism and the security of the global supply chain.[18] CSI extends our borders by stationing CBP officers at major international ports to pre-screen containers prior to their shipment to the United States. C-TPAT represents a genuine public-private partnership because private-sector applicants voluntarily commit to making security improvements in their supply chain in exchange for benefits from CBP.

In addition to these programs, CBP established the Radiation Portal Monitor Project to install radiation detection equipment at U.S. Ports of Entry to screen cargo, mail, and vehicles for radioactive materials upon arrival in the United States.[19] Another program to screen containers for radiation is the National Nuclear Security Administration (NNSA) Megaports Initiative, through which radiation detection equipment is provided to foreign governments and installed at major international seaports. Containers transiting these ports are screened by radiation detection equipment, effectively providing an additional layer of screening prior to the containers' arrival at a U.S. port. Collectively, these programs represent U.S. Government's efforts to secure the global supply chain and have been examined thoroughly in the Subcommittee's oversight investigation.

Shortly after the inception of CSI and C-TPAT, PSI commenced its oversight of these critical programs. During the course of its oversight investigation, the Subcommittee has raised significant concerns about the effectiveness of these programs. For instance, on May 26, 2005, the Subcommittee held a hearing entitled, "The Container Security Initiative and the Customs-Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?" That hearing examined the effectiveness of CSI and C-TPAT, and included the release of GAO audits concerning these programs. These audits, coupled with the oversight effort of the Subcommittee, revealed significant shortcomings:

- CBP inspects a *de minimus* number of containers overseas – 0.34 percent.
- Even worse, only 17.5 percent of high-risk cargo is inspected overseas.
- Equipment such as nuclear detection devices and Vehicle and Cargo Inspection System (VACIS) machines used overseas for inspections are untested and of unknown quality.
- Substantial benefits, including fewer inspections, are provided to certified C-TPAT importers without a thorough review or validation of their supply chain security procedures.

Although many of these problems have been addressed, significant challenges remain.

B. Container Security Initiative

The primary purpose of the CSI program is to protect the global supply chain through the placement of DHS personnel in foreign ports to target high-risk containers for inspection prior to their departure for U.S. ports. As of March 27, 2006, 44 foreign ports are CSI designated.[20] CSI teams stationed abroad generally consist of CBP officers and an Immigration and Customs Enforcement (ICE) agent.

Under this program, a team of CSI officers is deployed to work with host nation counterparts to target high-risk containers.[21] CSI was initially implemented at the top 20 ports by volume of shipping to the United States.[22] CBP has continued to expand this program with

---

[18] The U.S. Customs Service was merged into the Department of Homeland Security to form the U.S. Customs and Border Protection (CBP) in early 2003.

[19] The terms "radiation detection equipment" refers to Radiation Portals Monitors (RPMs).

[20] *See* Appendix B.

[21] The CSI team identifies high-risk shipments through ATS. After further analysis of the shipment, through document review and database checks, the CSI team may request the host country to examine particular shipments. If the host country officials decide against an examination of the shipment, or an examination is not possible because the container is already laden on board the ship, the CSI team will refer that particular shipment for an examination at the first U.S. port of entry.

[22] *See* CBP website, *http://cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml*,

the intent to deploy to 50 international ports by the end of Fiscal Year 2006.[23] CBP's strategic objectives for CSI include:

- Pushing the United States' zone of security beyond its physical borders to confront the threat of terrorism at its source;
- Targeting potential terrorists and terrorist weapons through advanced and enhanced information, intelligence collection and analysis, and preventing those shipments from entering the United States;
- Enhancing homeland and border security while facilitating growth and economic development within the international trade community; and
- Utilizing available technologies to leverage resources and to conduct an examination of all high-risk containers.[24]

Although a promising concept, PSI staff has identified several operational shortcomings with CSI. For example, CSI ports are unable or unwilling to inspect the quantity of containers necessary to significantly improve security. One reason for this, PSI has found, is that some CSI ports routinely "waive" the inspection of high-risk containers, despite requests by CSI personnel for an inspection. As a result, numerous high-risk containers are not subjected to an examination overseas, which undermines the primary objective of CSI. PSI has also identified other CSI ports that identify an inordinately small number of containers as "high-risk." Nonetheless, CBP has aggressively pursued the expansion of CSI without assessing the performance and productivity of its existing CSI ports.

1. Membership Process

A prospective CSI port must commit to a number of items before CBP will formulate an agreement with the host country. These minimum standards include: (1) the ability of CBP personnel to inspect cargo exiting or transiting their country; (2) access to and use of Non-Intrusive Inspection (NII) equipment; and (3) a willingness to share trade data and intelligence. Once the parties agree to these criteria, CBP executes a Declaration of Principle (DOP) with the host country to formalize the expectations each country has with the program. While the document is not legally binding, it is the formal document utilized by CBP to establish a CSI port. It appears from a review of these DOPs, however, that their purpose is to arrange for CBP personnel to be placed in a given country quickly, rather than to establish any minimum standards relating to the effective operation of a CSI port.

2. Areas of Concern

Some CSI ports are not complying with the minimum standards required by CBP. Those ports are either unwilling or unable to share intelligence, and some lack the ability to search the U.S.-bound cargo that was transiting their ports. The fact that certain ports are not adhering to these minimum and essential standards significantly undermines the purpose and effectiveness of the CSI program. After reviewing the DOPs that CBP executes with host countries, the Subcommittee found that these critical standards are not formally incorporated into these agreements. Although the DOPs explicitly reference examining high-risk containers, they contain no standards for NII equipment and do not require that the host country inspect high-risk containers, absent mitigating circumstances. Given the content, or lack thereof, of the DOPs, it is not surprising that the percentage of high-risk containers that are searched abroad is staggeringly low. Due to the weaknesses of these DOPs, CBP lacks an effective recourse to hold CSI ports accountable if they do not agree to inspect high-risk containers prior to debarkation.

(a) Minimum Standards for Equipment

According to CBP officials, CBP could not mandate specific NII or radiation detection equipment in connection with the CSI program because of sovereignty concerns, as well as restrictions that prevent CBP from endorsing a particular brand of equipment. Although CBP

---

accessed March 21, 2006.

[23] *Ibid.*

[24] *Ibid.*

claims that it cannot endorse a specific brand of equipment, the agency could nonetheless establish general technical capability requirements for any equipment used under CSI when signing the DOPs. Since the CSI inspection could be the only inspection of a container before it enters the United States, it is crucial that the nonintrusive inspection and radiation detection equipment used as part of CSI meets minimum technical requirements to ensure that the equipment could detect a WMD.

(b) Management and Staffing Challenges

CBP continues to face challenges in developing performance measures to assess the effectiveness of CSI targeting and inspection activities. In addition, CBP has not implemented a sound "red team" program to test the program's efficacy. Therefore, it is difficult to objectively assess progress made in CSI operations over time, and it is similarly difficult to compare CSI operations across ports. Staffing imbalances at CSI ports present an additional point of concern for CSI, especially at the highest-volume ports. Although CBP's goal is to target all high-risk U.S.-bound containers at CSI ports before they depart for the United States, CBP was initially unable to place enough staff at some CSI ports to do so. Many of these concerns and the challenges were identified in the May 2005 GAO report and have been corrected.[25] For example, CBP is now able to review all high-risk shipments transiting CSI ports and, at many CSI ports, CBP is able to review all shipments.[26] However, given the expense of CSI and sovereignty concerns of host nations, it is not practical for CBP to fully staff each CSI port. Even with a full complement of staff, CBP would have no assurance that the host country could keep pace with, or would want to conduct, these additional inspections.

THE NATIONAL TARGETING CENTER (NTC) AND VIRTUAL CSI

This is the centralized coordination center for all CBP anti-terrorism efforts. Staff of the NTC target incoming people and goods moving across the 381 official Ports of Entry to the U.S. The goal of the center is to deter or disrupt any terrorist efforts by stopping the movement of individuals, the flow of materials or money needed for such an operation. Targeters at the NTC also assist CSI ports in reviewing manifests and targeting high-risk shipments.

A Virtual CSI is also located at the NTC. To achieve a Virtual CSI, the Pakistani government agreed to screen containers and send the image immediately to the NTC for further review and analysis. The Subcommittee is encouraged by the concept and recommends that CBP expand this program to lessen the resource commitment at CSI ports.

CBP, however, should determine the minimum number of officers that must be physically located at CSI ports to carry out duties that require an overseas presence (such as coordinating with host government officials), as opposed to other duties that could be performed in the United States (such as reviewing manifests and databases). CBP has supplemented staff at the CSI ports with domestic officers stationed at the National Targeting Center.[27] According to CBP officials, CSI teams abroad may contact these NTC officers in the United States and request their assistance in targeting specific shipments. The NTC staff, after targeting the shipments, notifies the relevant CSI team of their results, including whether the shipments are high-risk and should be referred to the host government for inspection.

The use of CBP officers at the NTC demonstrates that CBP does not have to rely exclusively on overseas personnel, as required in its staffing model. Moreover, most officers at CSI ports do not have much interaction with host government officials. These domestic officers, in essence, serve as a force multiplier. For example, at the CSI ports inspected by PSI staff, CBP officials indicated that typically only one or two CSI team members interact with host customs officials. In consideration of the substantial expense of deploying an inspector abroad, CBP should reevaluate its staffing model.

While these problems raise concerns, CSI improved the level of U.S. safety. CSI has led to greater information sharing between CBP and host country customs officials. For example, CSI has resulted in a strong bilateral cooperation and international awareness regarding the need

---

[25] *See* GAO-05-187SU, "Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts," April 2005.

[26] This refers to a manifest review.

[27] For more information on the NTC, see the text box on this page.

to secure global trade. Also, with the discovery and seizure of shipments under CSI of automatic weapons, ammunition, and other falsely identified contraband, many foreign customs services that lack strong law enforcement capabilities are currently seeking additional legal authority to strengthen their ability to fight terrorism. For example, the World Customs Organization passed a resolution in June 2002 to enable ports in all of its member nations to begin to develop outbound targeting programs consistent with the CSI model.[28]

(c) Targeting Challenges

CBP faces considerable challenges in targeting inspections of containers. CBP officers stationed at CSI ports overseas are often located considerable distances from the port.[29] The CSI teams stationed abroad are focused on reviewing data in ATS, the system utilized to identify high-risk containers.[30] Following a review of the relevant data, CBP officers provide a list of high-risk containers to the host country customs officials for an examination. Domestically, a high-risk score in ATS triggers an automatic NII scan. In CSI ports, however, it merely requires a further review of information.

This aspect of the process raises considerable concerns with both ATS and the general objective of the CSI program. For instance, if a U.S.-bound container is identified as high-risk at a CSI port, it should be examined abroad just as it would be upon arrival in the United States. CBP, however, limits examinations at CSI ports to only those containers that are identified as high-risk due to terrorism concerns.[31] This restriction presents significant vulnerabilities in the CSI program since terrorist nexus indications may be difficult to detect simply from manifest data.

For example, consider a container identified as high-risk by the ATS system due to suspected drug smuggling. This container is well above the domestic threshold for an examination. Even though this container would be inspected at a domestic port, it will likely not be examined overseas, even though a drug smuggler may also be moving terrorist weapons.[32] If, on the other hand, CBP feels strongly that the same drug smuggler does not present a security risk, then the ATS system should be modified so the shipment would not be identified as high-risk in the first place.

CBP UNABLE TO VERIFY DOMESTIC EXAMS

If a high-risk container is not examined abroad, CBP insists that an exam occurs domestically. CBP, however, does not have any mechanism to confirm that these exams actually occur.

Exams conducted abroad consist primarily of a NII screen because CBP officers at CSI ports cannot require a container to be physically opened for inspection. Although CBP can recommend such physical inspections, the host country is not bound to agree to these recommendations, and thus, physical examinations of suspicious cargo may not occur until its arrival in the United States. Moreover, in some cases CBP officers are not allowed to be present during the NII screening, as called for in the DOP for the program, and are not even provided the NII image for review until the ship has already departed for the United States. CBP personnel recounted this situation to PSI staff when staff visited the Port of Le Havre, the Port of Shanghai, and the Port of Singapore.

---

[28] *See* World Customs Organization, "Resolution of the Customs Co-Operation Council on Security and Facilitation of the International Trade Supply Chain," June 2002, http://www.wcoomd.org/ie/en/Recommendations/recommendations.html, accessed March 22, 2006.

[29] At Le Havre and Shanghai, the CSI team is located 40 minutes from the port.

[30] ATS is further detailed in Section D.

[31] This CSI restriction, which was initially imposed by some host governments, has evolved into a CBP self-imposed restriction.

[32] The link between drug smugglers and terrorist organizations was discussed extensively at a Senate Judiciary Committee hearing on May 20, 2003, which was entitled "Narco-Terrorism: International Drug Trafficking and Terrorism – A Dangerous Mix." John P. Clark, then Interim Director, Office of Investigations, U.S. Immigration and Customs Enforcement, Department of Homeland Security, discussed narco-terrorist investigations, stating, "[T]he transportation organization that is paid to smuggle cocaine today may very well be contracted to smuggle instruments of terror tomorrow."

Mr. Clark specifically mentioned an ongoing investigation at a major U.S. seaport, where ICE Special Agents uncovered a practice of contraband being removed from international cargo prior to the entry process. The contraband in this investigation was heroin and cocaine, but it could have just as easily been a radiological or nuclear device. *See http://judiciary.senate.gov/testimony.cfm?id=764&wit_id=2112*, accessed March 21, 2006.

(d) Not All High-Risk Containers Are Examined

Overall, the vast majority of containers referred to host nations by CSI teams for examination are, in fact, inspected overseas.[33] However, most high-risk containers are not referred for exam in the first place.[34] Accordingly, only a *de minimus* number of high-risk containers are actually inspected abroad.

Some containers that are referred by CBP, however, are not inspected for two primary reasons. The first reason is that the host government has intelligence indicating that the referred containers are not high-risk. Second, operational limitations may prevent host governments from conducting inspections before they depart the port. For example, CSI teams had to waive inspections for some referred containers because the host government officials said they did not have the ability to inspect the containers, or the containers were already loaded on departing vessels, or the containers remained on the vessel while it was docked in the port. Other CBP referrals were denied by host government officials, generally because they believed the referrals were based on factors not related to security threats, such as drug smuggling. Denials such as these reveal that it is difficult to assess what risks may be terrorist-related, since a drug smuggler may also be smuggling terrorist weapons in the same container.

CLARIFICATION: MAY 2005 GAO AUDIT AND PSI

GAO accepted the CBP explanation of the difference between high-risk containers domestically and terrorism-related high-risk containers abroad. PSI staff continues to raise questions regarding the ability of CBP to delineate between high-risk and terrorism high-risk containers, and thus the different procedures implemented domestically and at CSI ports abroad.

If a host country refuses to perform an inspection before a container is shipped to the United States, the only recourse that CBP has at its disposal to ensure a container is inspected is to issue a "Do Not Load" Order. This order advises the carrier that the specified container will not be permitted to be unloaded in the United States until a time when any associated imminent risk to the container is neutralized. Once the risk is neutralized, the container is to be loaded back onto the carrier and placed on hold for a domestic examination.[35]

To date, of the high-risk containers inspected overseas, no WMD have been discovered. However, because the technology to detect the presence of chemical or biological agents does not yet exist and certain configurations of nuclear/radiological materials are difficult to detect via an NII image, CBP officials cannot be certain that no WMD have passed through a CSI port. If a WMD or other cargo of concern is detected during a CSI inspection, the host government is responsible for taking appropriate enforcement measures and disposing of the hazardous material.

The CSI team is also supposed to request domestic exams for shipments that were inspected overseas, but not to the satisfaction of the CSI team. Such circumstances would arise if there was a disagreement over the interpretation of the x-ray image or if the host nation was not willing to perform a physical exam after an anomaly had been detected.

This additional inspection raises two other problems with CSI. First, in light of the fact that the essential purpose of CSI is to conduct inspection of high-risk containers *before* they enter U.S. ports, the examination of these high-risk containers upon arrival in the U.S. undermines the central objective of the CSI program. Moreover, after the targeted container has arrived at the U.S. port, CBP cannot effectively demonstrate whether that container was subsequently inspected in the United States.

---

[33] According to data supplied to the Subcommittee by CBP, 82.7 percent of exams requested at all CSI ports from February 2005 to February 2006 were conducted.

[34] According to data supplied to the Subcommittee by CBP, only 37.24 percent of high-risk shipments were examined. Out of the 143,853 high-risk shipments identified by ATS, only 69,543 exams were requested by CBP at CSI ports in 2005.

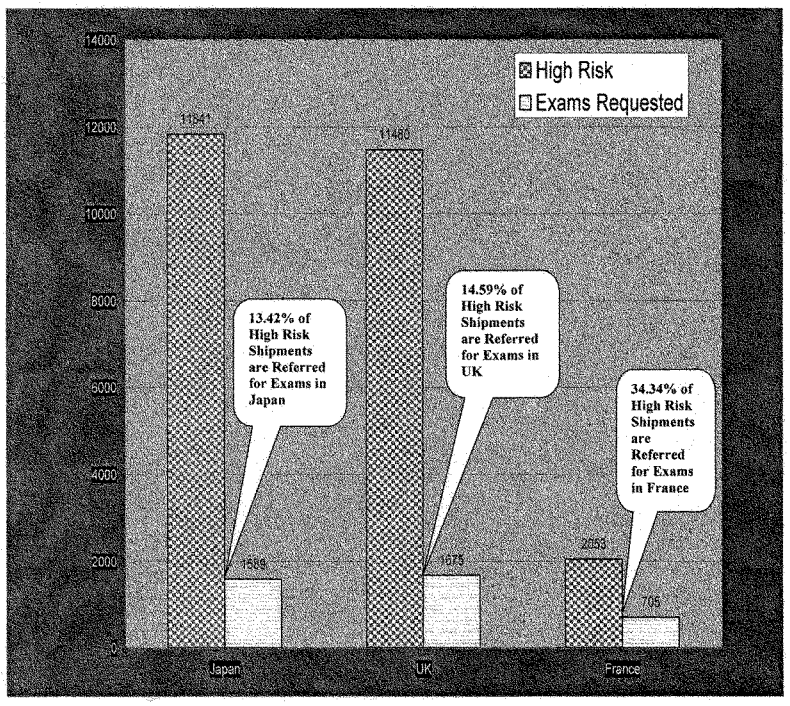
[35] CBP has never issued this order for security reasons; however, they have issued these orders for violations of the 24-hour rule.

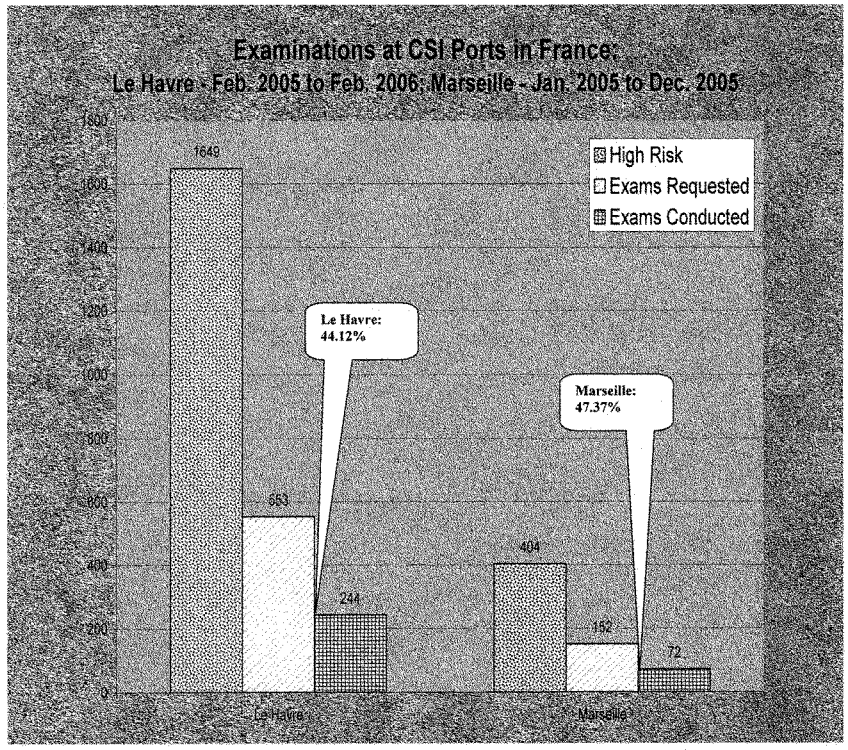
(e) Low Inspection Rates at CSI Ports

The rate of inspections of high-risk containers is disturbingly low. To illustrate the *de minimus* number of inspections, the Subcommittee has prepared case studies for the CSI ports in the United Kingdom, Japan, and France. Unfortunately, the numbers tell a troubling tale. These cases studies expose two significant problems related to the inspection rates of high-risk containers under the CSI program.

(i) CBP Refers a Fraction of High-Risk Containers for Inspection

First, the data reveals that CBP is referring only a fraction of containers that have been identified as high-risk for examination. For instance, in the U.K., CBP referred for inspection only 465 out of 2480 containers that had been identified as high-risk – amounting to an inspection rate of only 14.59 percent. CBP referred only 34.34 percent of high-risk containers transiting French ports for inspection. The lowest rate of referral occurred in Japan, where CBP submitted only 13.42 percent of high-risk containers. This data is especially disturbing in light of the fact that the countries at issue are among America's closest allies, which would presumably work cooperatively with CBP. The graph presented below illustrates the dramatic gulf between the number of high-risk containers and the number of inspections requested by CBP.

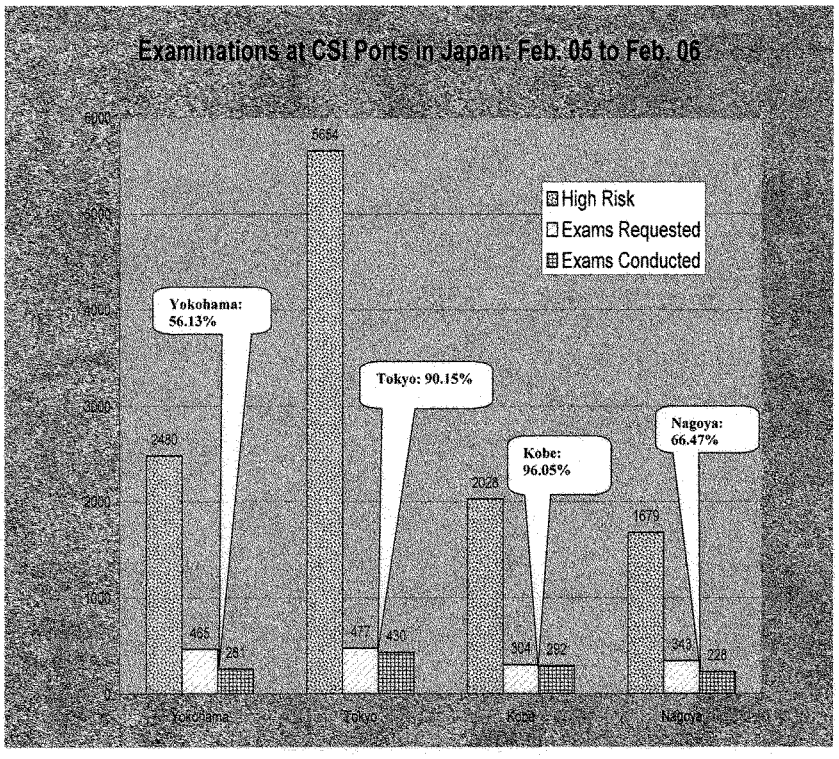




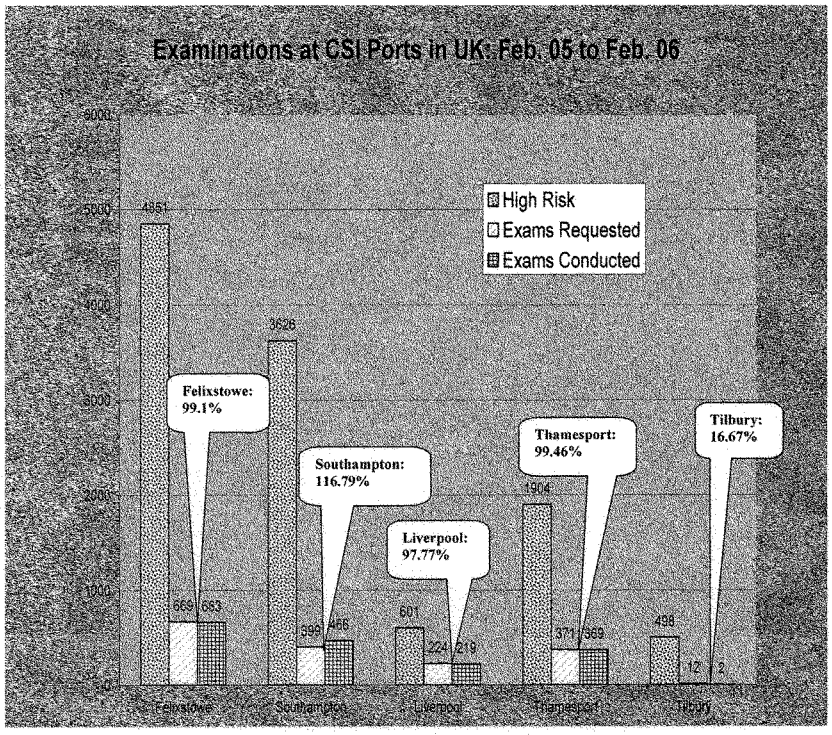
(ii) Inspection of CBP-Referred Containers Is Inconsistent

Beyond the fact that CBP refers only a fraction of high-risk containers for inspection, the Subcommittee's case studies reveal a second significant problem – host countries fail to inspect a substantial number of CBP-referred containers. For instance, of the 705 examinations that CBP requested from French authorities, only 316 inspections were conducted – a rate of only 44.82 percent. The rate of inspections of high-risk containers at each CSI port in France is reflected in the figure below.

In Japan, CBP requested inspections of 1,589 high-risk containers from February 2005 through February 2006. Of the 1,589 requested inspections, 1,211 examinations were conducted – a rate of 76.21 percent. The rate of inspections of high-risk containers at each CSI port in Japan is reflected in the figure below.



In contrast with the low inspection rates in Japan and France, the percentage of CBP-requested examinations that are ultimately conducted in the U.K. is quite high. In fact, the case studies reveal that U.K. officials inspected 100 percent of all containers that are referred by CBP from February 2005 through February 2006. Indeed, in some cases, the U.K. authorities actually examined additional containers beyond those requested by the CSI teams in the U.K. This data is reflected in the figure below.



In sum, these cases studies reveal profound flaws in CSI's inspection regime. The data suggests that CSI teams at the ports in France, Japan and the U.K. refer a disturbingly low percentage of high-risk shipments for exams. This may reflect a problem with the risk targeting system, called ATS, which is discussed in Section D of this report. In particular, ATS may be identifying too broad a spectrum of high-risk containers and therefore does not effectively delineate high-risk shipments. Aside from problems underlying ATS, CBP attributes the low inspection rates at CSI ports to: (1) mission fatigue; (2) lack of resources and time; and (3) mistrust in the targeting system that identifies high-risk containers.[36] However, CBP does emphasize that these countries would examine a container if CBP had grave concerns about a particular container. The Subcommittee believes CBP's statement demonstrates the very shortcoming of the targeting system. We cannot rely on this targeting system to accurately identify the genuine terrorist-related containers, and as such, *all* high-risk containers need to be examined abroad, not just the select few that are referred by the CSI team to the host country.

3. Staff Trip and Observations

Since 2003, PSI staff has conducted four oversight trips to ten CSI ports in Europe and Asia to further examine these programs in practice. The observations at the following ports significantly contributed to the Subcommittee's investigation.[37]

---

[36] CBP meeting with Subcommittee staff on March 16, 2006.

[37] Observations by Subcommittee staff consisted of half-day examinations of port operations at each facility.

(a) Port of Rotterdam: The Netherlands (December 2004)

The Port of Rotterdam, which is one of the world's ten largest ports, was the first international port to enter the CSI program. The CSI team on-site in Rotterdam is permanent, consisting of three targeters, one intelligence analyst, one ICE agent, and one supervisory team leader. While this team appeared to be effective, members of the CSI team agreed that a smaller liaison capability in Rotterdam, coupled with a team of dedicated targeters examining bills of lading in the United States, would also be successful. The Port of Rotterdam uses a nine Mega Volt NII (X-ray) machine to examine cargo. As a point of comparison, the imaging machine used in the United States emits less than one mega volt. The higher level of megavolts used in Rotterdam allows for a better and more accurate scan.

The Port installed RPMs, through the Megaports Initiative, configured with a relatively low radiation threshold. This low threshold results in 100-200 alarms per day. Dedicated analysts examine the output of the scan and, pending their analysis, direct certain cargo to a secondary inspection area where they are examined with a handheld radiation scanner. According to officials in Rotterdam, these scanners do not slow down traffic or cause delays at the Port.

Operations at the Port of Rotterdam and the cooperative effort with Dutch Customs were impressive. The success of the CSI program may be attributed to the localized database, entitled CSI-NT (a subset of ATS), which was specifically configured for testing containers transiting through Rotterdam and enhances the targeting ability of the CSI team. This specialized subset of ATS, CSI-NT, has proved to be effective in improving targeting and should be incorporated and expanded to programs at other major ports.

(b) Port of Le Havre: France (December 2004)

The Port of Le Havre illustrated the numerous challenges confronting the CSI program. According to French Customs, French law requires the government to pay a $100 surcharge to a company whose container is inspected. Although French officials assert that the surcharge has no impact on their inspection rates and their ability to inspect containers referred by the CSI team, the CSI team in that port disagrees. The CSI team and CBP believe that this surcharge does in fact affect the French determination of whether to inspect containers, and negatively impacts their inspection rates. Indeed, inspection rates from the Port of Le Havre are particularly low, as denoted earlier in the report.

France uses a five megavolt Heimann CargoVision scan in three different screening bays as part of its NII program. The French plan to add radiation screeners to these bays, which will allow for simultaneous radiation screening and NII. After the addition of radiological screening equipment, the only containers that will be inspected for radiation prior to loading will be those containers that warrant additional inspections. This planned process is flawed in that it presumes that radiation material will be smuggled in a container that warrants additional inspections. However, given that the primary concern of French inspectors is cigarette smuggling, the targeting of screening will be misdirected and too narrowly focused. In sum, the current system of inspections portends many challenges for the French to successfully detect the smuggling of radiological material.

While the CSI staff in this port is permanent and appeared to be establishing strong relationships with local French Customs officials, the visit to Le Havre illuminated many of the challenges confronting the CSI program, from the reliability of the C-TPAT program, to the rationale for six in-country CBP personnel to the limited inspection rates to the inability to screen for radiation.

(c) Port of Felixstowe: United Kingdom (December 2004)

CSI staff indicated that they reviewed all bills of lading of cargo transiting through the Port of Felixstowe to the United States, yet made few requests for inspections by Her Majesty's Customs and Excise. Additionally, CSI staff indicated that they believe that the ATS system requires considerable modifications, and as a result, they view a high-risk score in ATS merely as an additional piece of information and a precursor for added research to gauge whether an inspection is necessary. Moreover, the CSI staff did not contact the NTC for additional assistance in their targeting because "they did not want to bother" NTC staff. Overall, the CSI team in Felixstowe demonstrated that a lack of knowledge, resources, and inspections may in

fact be adding to the cargo security challenge. CBP officers at major U.S. ports have told PSI staff on several occasions that they view containers arriving from a CSI port with less scrutiny than those originating in non-CSI ports. This indicates that operations at CSI ports must be standardized to ensure that high-risk containers are inspected at a CSI port, or domestically.

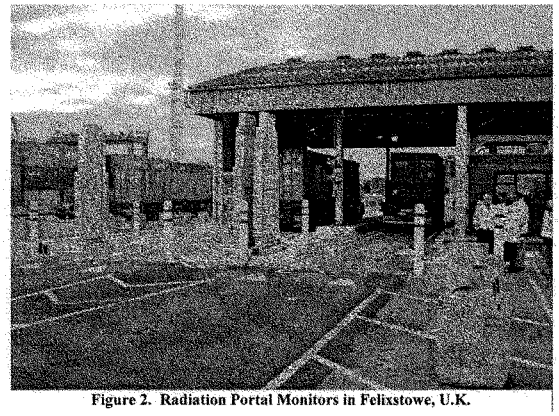


Figure 2. Radiation Portal Monitors in Felixstowe, U.K.

(d) Port of Hong Kong: Special Administrative Region of China (August 2005)

As the world's busiest port, Hong Kong was one of the first ports to enter CSI. At the time of the initial staff trip to Hong Kong in August 2004, Subcommittee staff observed that the CSI team was not able to review 100 percent of manifests. This was primarily due to the lack of staffing resources.[38] These problems have been largely fixed. Today, the CSI team reviews 100 percent of manifests and utilizes CBP officers at the NTC to accomplish this goal. In addition, Hong Kong Customs has established a specialized targeting system to assist the CSI team. This system extracts manifest information from ATS and links that data to the Hong Kong targeting systems. By utilizing both of these systems, the CSI team in Hong Kong has improved their targeting capabilities. PSI has observed an exceptionally positive relationship between Hong Kong Customs and CBP during their oversight trips to Hong Kong.

(e) Port Klang: Malaysia (August 2004)

The visit to Port Klang highlighted the importance of training staff to effectively operate NII equipment. Figure 3 is an image of a CSI-referred container from Malaysia that illustrates PSI concerns with these images. The image is black. When asked what he was screening, the Malaysian inspector stated rugs. When asked how he could discern rugs in the image, he replied that while he could not see anything in the image, rugs were indicated on the manifest. This exchange shows the limitation of technology and how that can defeat the whole purpose of scanning the containers.

[38] In May 2005, the GAO reported that, according to the CSI staffing model, the appropriate number of targeters for the Port of Hong Kong is 21. However, only eight targeters were assigned to the Port, and as of September 11, 2004, only 30 percent of U.S.-bound shipments from that Port had been targeted.

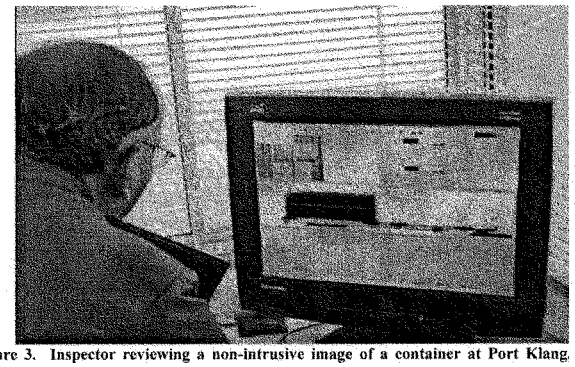


Figure 3. Inspector reviewing a non-intrusive image of a container at Port Klang, Malaysia

4. Recommendations

In sum, CSI was and remains the right idea for post-9/11 security. Nevertheless, effective CSI implementation is fraught with challenges. As such, the Subcommittee staff makes the following recommendations:

- The targeting system – ATS – must be adjusted to effectively identify high-risk containers.
- The use of a specialized subset of ATS, such as in Rotterdam, must be expanded to other CSI ports.
- The number of inspections conducted abroad needs to increase dramatically.
- The arbitrary distinction between high-risk cargo due to narcotic smuggling and high-risk cargo due to terrorism is difficult to identify and may demonstrate a potential vulnerability.
- The Virtual CSI program is an innovative concept that must be expanded, especially if coupled with the Hong Kong Screening Model or equivalent technology, which is discussed below.
- The CSI program should focus on improving inspection rates at existing CSI ports, prior to expanding to other ports.
- CSI targeting can be conducted domestically. CBP should readjust its staffing model and utilize a combination of officers in-country and at the NTC.
- Standards for inspections and technology must be incorporated into the DOPs signed by the United States and host governments to establish a CSI port.

C. Customs-Trade Partnership Against Terrorism

Another vital layer in CBP's security strategy is the Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT was rolled out as an initiative shortly after the September 11th attacks and then Customs Commissioner Robert C. Bonner described it as "a lasting partnership between Customs and industry to ensure both security for our Nation, and the smooth flow of commerce across our border."[39] C-TPAT aims to secure the flow of goods bound for the United States by developing a strong, voluntary antiterrorism partnership with the trade community.

---

[39] Robert C. Bonner, Commissioner of U.S. Customs Service, speech announcing C-TPAT, April 16, 2002, Detroit, Michigan, *http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/archives/2002/apr162002.xml*, accessed February 9, 2006.

To participate in C-TPAT, private sector companies commit to improving the security of their supply chains. In exchange for this commitment, CBP will grant C-TPAT members a range of benefits, many of which are designed to reduce CBP's level of scrutiny of the members' U.S.-bound shipments. Foremost among these benefits is a reduction in risk score for their imports in CBP's targeting system, which assigns a risk to a shipment based on factors such as whether the shipment is coming from a country with terrorist ties.[40] Lowering the risk score will, in turn, reduce the probability of extensive documentary and physical inspection of members' shipments, and will facilitate the rapid movement of their cargos. Among all the benefits offered to program members, this reduction in risk score is clearly the most cherished since it reduces the number of inspections a shipper must endure. Other benefits of C-TPAT include:

PREVIOUS PROBLEMS

When CBP initiated C-TPAT in 2002, it granted the benefits of participation to C-TPAT applicants immediately upon receipt of their agreement to participate in the program. Importantly, CBP would grant these significant benefits after only a cursory review of the applicant's security plan – and before CBP had conducted any assessment of the applicant's proposed security profile. CBP eventually recognized the weaknesses of this process, and revamped the C-TPAT membership process. The current process, which was launched in May 2005, is described in this report.

- CBP will reduce the number of inspections for that company's cargo, and will reduce the wait-time at the border for that company's shipments;
- CBP will assign a specific C-TPAT supply chain specialist to serve as the liaison to that C-TPAT member in order to facilitate validations, security issues, procedural updates, communication and training;
- C-TPAT members are given greater authority to police and monitor their own security activities; and
- C-TPAT certified importers receive reduced selection rate for Compliance Measurement Examinations and exclusion from certain trade-related local and national criteria.[41]

C-TPAT membership is open to U.S. importers of record, U.S./Canada highway carriers, U.S./Mexico highway carriers, air/sea/rail carriers, U.S. port authority/terminal operators, U.S. air freight consolidators, ocean transportation intermediaries, non-vessel operation common carriers, Mexican manufacturers, certain invited foreign manufacturers, and licensed U.S. Customs brokers. As of February 1, 2006, 10,434 companies have applied for C-TPAT membership and 5,777 companies have been accepted and "certified."[42]

1. Membership Process

CBP employs a two-pronged approach to assess C-TPAT applicants before granting C-TPAT benefits. First, CBP conducts a review of the self-reported information contained in an applicant's membership agreement and security profiles and assesses the applicant's compliance with customs laws and regulations, history of violations, and intelligence data. Following a successful review, the applicant is deemed certified by CBP. Certification also provides for the company to be eligible for a validation, which is the next stage of review. The current membership process, including the tiered benefit structure, is described in detail below.

(a) Certification

The C-TPAT process begins with an applicant completing a comprehensive security self-assessment or profile, outlining in detail how the applicant is meeting certain defined minimum security criteria. A Supply Chain Security Specialist (SCSS) will then review the submitted profile to determine whether the applicant satisfies the minimum security criteria. These

---

[40] This risk-targeting system, called ATS, is examined in detail below.

[41] *See* "Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan," CBP, *http://cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf*, accessed February 7, 2006.

[42] The term "certified" refers to the CBP certification process, in which the applicant has passed an initial review by CBP and is eligible for certain benefits. This process is discussed in great detail below. This data was supplied to the Subcommittee by CBP in March 2006.

minimum security criteria are determined by CBP and include whether the company conducts background checks of employees, whether the applicant's facilities are secured by a fence, and requires that the C-TPAT member work with other C-TPAT members. Approximately 20 percent of initial submissions are rejected for failing to meet the minimum security criteria.

Concurrent with the security profile review by the SCSS, C-TPAT officers vet the applicant through CBP law enforcement and trade databases, as well as the El Paso Intelligence Center. Companies must be free from past narcotics or serious trade violations before being accepted into the program. Other disqualifying factors include involvement in human smuggling incidents, having been the subject of criminal investigation, having associations with known criminal organizations, involvement with illegal transshipment schemes, and violations of intellectual property rights. In addition, the company must have a demonstrated import history of a minimum number of shipments into the United States before acceptance into the program.[43]

If an applicant satisfies these requirements, the company is considered "certified" and accepted into the program and eligible for Tier 1 benefits, which include a reduced score on CBP's risk-targeting system. In addition, the company becomes eligible for the second level of review, called validation, which provides additional benefits.

(b) Validation

The validation process is designed to ensure that the security practices outlined in the applicant's security profile are in place and effective. If an applicant's security apparatus satisfies certain minimum security criteria, it becomes eligible for Tier 2 benefits. Companies whose security practices exceed the minimum security criteria, however, are eligible for even greater privileges, called Tier 3 benefits. The validation process is primarily focused on importers and carriers, which are generally in the best position to induce security enhancements deep into the international supply chain.

CBP prioritizes which certified companies to validate based on risk. CBP uses a risk assessment tool – the Quantitative Risk Assessment Module (QRAM) – to determine a quantifiable risk score for each certified member.

VALIDATIONS

Only one supply chain for each C-TPAT member will be validated, even if that company uses hundreds of supply chains. This represents another potential vulnerability as an importer that utilizes supply chains across the world will only have one of these supply chains validated. CBP, thus, has little insight into if the company's practices in other countries are as secure.

The validation process is generally conducted by two SCSS. Each validation begins with a visit to the domestic corporate office of the member. At this initial meeting, the SCSS review the company's security profile utilizing a standard 900-question automated tool. The SCSS, usually accompanied by representatives of the C-TPAT member, complete a review of the member's supply chain security. CBP will also indicate at this meeting which of the company's supply chains has been selected for validation.

After the initial meeting, the SCSS will conduct a foreign site visit to examine the company's security practices. This review focuses on the company's operations at point of stuffing, during transit to the port of debarkation, and at the foreign port itself. Upon conclusion of the domestic and foreign review, CBP and the applicant hold a closeout meeting to discuss the findings, required actions, and all recommendations. A final written report is also provided to each validated company a short time after the closeout meeting.

The final written report is reviewed by the C-TPAT Director, who makes the determination as to whether the member is meeting the minimum security criteria and thus is eligible for Tier 2 benefits, or is exceeding minimum security criteria and employing best practices, and therefore eligible for Tier 3 benefits.

(c) C-TPAT's Tiered Benefit Structure

CBP adopted a tiered benefits structure for C-TPAT in May of 2005. As noted above, a company that has been certified – but not validated – is eligible for Tier 1 benefits. Tier 1

[43] CBP has defined the minimum number of required shipments but does not disclose this number to the public.

benefits, the lowest level under C-TPAT, include a reduced score on CBP's risk targeting system.[44] C-TPAT members in Tier 1 also enjoy other privileges. Members are eligible to participate in the Importer Self-Assessment Program administered by the Office of Strategic Trade, attendance at CBP-sponsored training seminars, and access to the Automated Commercial Environment portal. C-TPAT certification is a prerequisite for eligibility to participate in the Free and Secure Trade program. As of February 1, 2006, 2,429 importers were certified and eligible for Tier 1 benefits.[45]

Companies satisfying CBP's minimum security standards are eligible for Tier 2 benefits. Tier 2 benefits include all the privileges of Tier 1, with two significant additions. First, the reduction in CBP's risk targeting system for Tier 2 members is even larger than that of Tier 1. In addition, companies eligible for Tier 2 benefits enjoy "front of the line" privileges, meaning that, if inspection was required, their cargos receive expedited treatment. Only 553 importers have been validated and found to meet the minimum security criteria, making them eligible for Tier 2 benefits.[46]

Companies that maintain security arrangements that exceed the industry's best practices receive even greater privileges, called Tier 3 benefits. Those benefits include all the advantages of Tiers 1 and 2. Perhaps most important, Tier 3 companies receive an even greater reduction in the risk targeting system. Tier 3 companies also enjoy the expedited, "front of the line" treatment for inspections. As of February 1, 2006, only 139 importers have achieved Tier 3 status.[47]

2. Problems With C-TPAT

As described above, CBP employs a two-pronged process to certify and validate applicants to the C-TPAT program. CBP officials have indicated that this two-pronged approach is adequate to ensure the security of the applicant's supply chain. CBP's confidence, however, may be overstated for two reasons. First, C-TPAT benefits are provided to importers after only reviewing self-reported information. Second, while the validation process for C-TPAT members is a more in-depth analysis of security practices, that heightened process examines only one supply chain for each participant.

3. Recommendations

The Subcommittee staff makes the following recommendations:

- The validation process needs to be strengthened to include a review of additional supply chains.
- A revalidation strategy must be developed and validations must be conducted for each C-TPAT member with a clear strategy and timeline for completing the validations.
- CBP should work collaboratively with C-TPAT members to develop self-policing standards.
- CBP must consider the use of third-party entities to validate C-TPAT members.

D. Automated Targeting System

Over the past several years, PSI staff has examined CBP's methods to target and subsequently search high-risk shipping containers for weapons of mass destruction, counterfeit goods, stowaways, and other forms of contraband. The primary tool deployed in CBP's effort to target high-risk containers is the Automated Targeting System (ATS).

ATS is a collection of rules that allow CBP officers to target inbound containers based upon manifest information, entry data, intelligence inputs, and other automated rules developed by CBP. The rules are applied to every shipment and re-applied when new information is

---

[44] Notably, the score reduction benefits in ATS apply only to importers and are provided only upon the receipt of entry data.

[45] This data was supplied to the Subcommittee by CBP in March 2006.

[46] *Ibid.*

[47] *Ibid.*

obtained or updated. After the application of the rules, the values assigned to each rule are tallied and the final result is the targeting score. CBP officers using ATS are, in theory, able to rank containers by risk, then conduct further analysis to determine whether a suspect container should be inspected (either a physical or a non-intrusive image examination) before the shipment is granted U.S. entry. ATS was originally designed to help identify illegal narcotics in cargo containers, but after the terrorist attacks of 9/11, was modified to identify all types of contraband that might be smuggled by terrorists. As noted by CBP's website:

> ATS ... is a system that [assists] Customs officers in identifying imports which pose a high risk of containing narcotics or other contraband. This program is a joint effort by the Office of Field Operations and the Office of Information and Technology.... The system standardizes bill-of-lading, entry, and entry summary data received from the Automated Commercial System (ACS) and creates integrated records called "shipments." These shipments are then evaluated and scored by ATS, through the use of over 300 weighted rules derived from targeting methods used by experienced Customs personnel. The higher the score, the more the shipment warrants attention.[48]

ATS is the foundation of the layered security strategy employed by CBP in its fight against terrorism and the smuggling of radiological or nuclear weapons. If ATS does not effectively identify high-risk containers, it may undermine one of the principle objectives of CSI – inspecting high-risk containers before they reach U.S. ports.

1. Areas of Concern

ATS may have some value in assisting CBP officers in identifying imports that pose a high risk of containing narcotics or contraband, as ATS was originally designed to identify narcotics contraband. [49] Nevertheless, many questions remain as to both the degree to which this system is capable of accomplishing that task and the extent to which ATS is increasingly relied upon as the primary tool for determining which containers should receive an inspection. An inspection (whether through the total removal of a container's contents, or a non-intrusive image examination) is the agency's most exhaustive tool to discover WMD or other contraband. However, inspections are mandatory only for high-risk containers. An inspection is unlikely if ATS does not designate a container as high-risk. Thus, if ATS fails to designate a container as high-risk, the chance of discovering whether a container houses a WMD is remote. It is therefore imperative that ATS be reliable and effective.

24-Hour Rule

The 24-hour Advance Vessel Manifest Rule was issued on December 22, 2002 in response to a provision in the Maritime Transportation Security Act (MTSA). The 24-hour rule requires detailed information on the contents of sea containers bound for the U.S. be transmitted 24 hours before the container is loaded on board a vessel. Containers bound for non-U.S. ports that transit through a U.S. port must also comply with this rule. Sea carriers and Non-Vessel Operation Common Carriers (NVOCCs) must provide this information to CBP; violations of this rule will result in a "Do Not Load" message from CBP and denied permission to unload the container at any U.S. port. Egregious violations of timeliness rules will result in monetary penalties. This rule was enacted to give CBP an opportunity to review the contents of a container prior to the container being loaded on board a vessel. With the advance receipt of the information, CBP can target high-risk containers.

See CBP website, *http://www.cbp.gov/xp/cgov/newsroom/press_releases/archives/cbp_press_releases/022003/02132003.xml*, accessed March 27, 2006

Challenging the system from the outset is the reliance on manifest data as the essential piece of information to calculate risk.[50] Members of the international trade community and CBP

---

[48] *See* CBP website, "Automated Targeting System," U.S. Customs and Border Protection, *http://www.cbp.gov/xp/cgov/import/operations_support/automated_systems/automated_targeting_system.xml*, accessed February 7, 2006.

[49] *See* GAO-04-352NI, "Homeland Security: Challenges Remain in the Targeting of Oceangoing Cargo Containers for Inspection," February 2004, p. 20.

[50] The term "manifest data" refers to customs documents listing all contents aboard a particular vessel, in particular cargo, crew and/or passengers.

officers characterized the manifest as the least reliable form of data for targeting purposes, as it is subject to errors and inaccurate information.[51]

Moreover, as described earlier, one of the vulnerabilities is the overseas portion of the supply chain, where goods are loaded into containers at consolidation centers. The company that loads or "stuffs" the container is most often a third party and the identity of this third party is not listed on the manifest. ATS, however, relies almost exclusively on the manifest information, and therefore does not take into account the identity of the third party.

CBP officers and even members of the trade community have urged CBP to require the submission of additional information beyond the manifest data. For instance, CBP officials use entry data when it is available to supplement the manifest data, as entry data is considered more reliable and accurate. Entry data, however, is not required to be filed prior to the vessel loading, and is sometimes not filed until after the arrival of the cargo. It is also worth noting that C-TPAT score reductions in ATS do not apply unless entry data has been filed.[52]

Another weakness with ATS is the lack of simulated tests or so-called "red teams" on the system, except for the two instances by ABC News in 2002 and 2003. ABC News simulated a terrorist smuggling highly enriched uranium into the United States. ABC News placed depleted uranium in a lead-lined pipe, sealed the pipe and transported it in a suitcase that was later placed in a cargo container. In both cases, CBP targeted the container, but after using non-intrusive inspection equipment, did not detect a visual anomaly and, as a result, did not open the container.[53]

CBP does randomly select and examine containers, but these random inspections can be waived if the resources are needed to conduct ATS or other intelligence–driven inspections. Additional concerns with ATS include:

- ATS has yet to be peer reviewed, red-teamed or validated through simulated events to demonstrate that it identifies high-risk shipments.
- ATS cannot incorporate real-time information or adjust dynamically.
- CBP is unable to fully use inspection data. This prevents CBP from evaluating the efficiency of ATS based on the results of cargo inspections. CBP officials stated that an enhancement to ATS called the findings module to allow CBP to review what was found in each container inspected would be available in November 2003. As of today, this ATS findings module is still not operational.[54]

2. Staff Observations

PSI staff has frequently observed that a container's initial risk score generated by ATS is the primary tool of CBP officers to determine whether that container should be referred to a host inspectorate for physical examination. Nonetheless, it remains unclear whether a high ATS score realistically correlates with the actual risk. Notably, only one of the containers used in the smuggling incidents involving Chinese immigrants at the Port of LA/LB in January and April of 2005 were identified as high-risk by ATS.[55] This failure demonstrates the inherent limitations of relying upon a risk management tool that has not been tested, validated, or red-teamed. In addition, other questions that arise, such as whether containers categorized as "high risk" by ATS carry more contraband (and thus possibly a WMD) than randomly selected containers; whether CBP has statistical evidence that validates that claim; whether CBP considers that the general

---

[51] *See* GAO-04-352NI, "Homeland Security: Challenges Remain in the Targeting of Oceangoing Cargo Containers for Inspection," February 2004, p. 26.

[52] This is an important distinction because entry date is not normally filed until a few days prior to arrival in the United States. Therefore, C-TPAT importers rarely receive any score reductions in ATS at CSI ports since entry data is not yet available.

[53] *See* GAO-04-352NI, "Homeland Security: Challenges Remain in the Targeting of Oceangoing Cargo Containers for Inspection," February 2004, p. 28.

[54] On March 10, 2006, GAO auditors updated PSI and HSGAC staff on the ongoing audit of ATS. GAO auditors informed staff that the ATS findings module was still not operational.

[55] During these two separate incidents, illegal Chinese aliens were discovered in ocean containers at the Port of Long Beach. The containers were transshipped from a CSI port and carried by a C-TPAT member.

category of contraband, whether stowaways or drugs, serves as a surrogate for WMD for purposes of evaluating this program, and if not, what variables it would use in this regard.

On repeated occasions, PSI staff has queried Customs officials regarding the potential over-reliance on ATS, particularly to determine which shipments should be examined for potential WMD. Moreover, the PSI staff remains concerned that, without some indication that ATS significantly assists CBP as a tested and validated risk management tool, CBP will continue to rely on ATS as the primary tool for keeping dangerous goods – including a WMD – from entering the U.S.

3. Recommendations

Because ATS is the foundation of U.S. Government supply chain security programs and given the considerable challenges that confront this program, the Subcommittee staff makes the following recommendations:

- ATS must be scientifically assessed and proven to accurately identify high-risk containers.
- CBP should come to resolution with the trade industry in its discussions of additional data elements useful in targeting and implement plans to obtain and utilize that data, which may include entry data submitted prior to vessel arrival.
- CBP should develop procedures to facilitate the filing of entry data prior to the arrival of the vessel at a U.S. port.
- CBP should establish baseline performance measures to evaluate the effectiveness of ATS as a targeting system.
- ATS rules need to be flexible and take into account findings from other high-risk cargo examinations and intelligence, as well as local factors.
- Simulated and red-team testing must be conducted on ATS.

E. The Radiation Portal Monitor Program [56]

Preventing a terrorist organization from acquiring and detonating a nuclear or radiological dispersal device in the United States is one of our nation's top priorities. To address this threat, CBP established the Radiation Portal Monitor Program (RPMP) in early 2002 to deploy Radiation Portal Monitors (RPMs) in U.S. Ports of Entry (POE). CBP has successfully deployed RPMs across the major crossings at the Northern and Southern Border, as well as at Express Consignment Carrier Facilities, to screen incoming packages. However, deployment at our nation's seaports – the very location where many experts believe a terrorist may try to smuggle a weapon – has been sluggish at best.[57] Four and half years after the September 11th attacks, less than 40 percent of incoming maritime containers are screened for radiation. Of additional concern are the skyrocketing costs of this program. The cost of the RPMP has escalated from $500 million to close to $1.5 billion, primarily due to a move towards a new type of nuclear detection equipment.

To bolster the effort to detect nuclear and radiological devices, DHS established the Domestic Nuclear Detection Office (DNDO) on April 13, 2005. The DNDO is tasked with addressing the threat of nuclear terrorism by coordinating nuclear detection activities, constructing a global nuclear detection architecture, and enhancing nuclear/radiological capabilities and technologies across the Federal Government. In addition to moving towards advanced radiation detection equipment, DNDO has sponsored research and development into additional technologies that would improve the ability of currently-fielded radiation detection equipment to distinguish between radiological sources.

---

[56] Staff is aware of the inherent limitation of radiation detection equipment, however, believes that radiation detection equipment, properly configured, enhances our collective security against the threat of radiological or nuclear terrorism.

[57] *See* GAO-06-389, "Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain," March 2006, p. 13.

1. Problems with RPMP

(a) Delayed Deployment

As of March 2006, DHS had deployed only 30.8 percent of the projected Radiation Portal Monitors.[58] Specifically, only 740 of the required 2,405 monitors have been deployed. The deployment is behind schedule, at some locations, by roughly 20 months.

The delays are caused by a wide array of problems including cumbersome funding procedures, setbacks in reaching necessary agreements with the terminal operators, difficulties in the screening of rail cars, weather, and construction problems. Some of those problems are detailed below:

- The funding for the RPM deployment is hampered by multiple layers of review and CBP's appropriations legislation requires that, prior to deployment, Congress review a spending plan prior to the deployment.
- Seaport operators have been reticent to sign agreements to deploy RPM equipment because they believe that the equipment will lead to more alarms and secondary inspections, thereby impeding the flow of commerce through their ports.[59]
- The screening of rail cars presents a challenge because the logistics of conducting a secondary inspection may obstruct rail traffic within the port, to the point of disrupting rail schedules throughout a broad geographic region. Such a disruption could potentially cost the port thousands of dollars per hour in lost revenue.[60] Another factor adding to the delay is that some ports do not have sufficient space to accommodate trains for the required secondary inspections. This issue will be magnified in the future as rail traffic is expected to double over the next 15 years with the Department of Transportation predicting that the amount of freight transported by rail will increase to 699 million tons by 2020.[61]

(b) Technological Problems and Rising Costs

Currently deployed equipment is unable to distinguish between naturally occurring forms of radiation and radiation of concern. This limitation has resulted in either a high rate of alarms or a high detection threshold, which allows containers to continue to move through the point of entry. These radiation portals that are able to identify radiation and cost approximately $70,000. CBP is planning to deploy advanced portals that can distinguish between naturally occurring radiation and radiation of concern, yet these portals cost more than four times as much as the other portals. Due to efforts of the Subcommittee, DHS has adjusted its deployment plan and will utilize a mix of these portals to ensure that radiation is detected, yet the costs remain manageable.

2. Observations and Findings

To view the progress and effectiveness of the RPMP deployment, PSI staff visited the DNDO Countermeasures Test Beds at the Port of New York/New Jersey. (See Figure 7, below) The RPMP program has approximately 200 radiation alarms on a daily basis with the majority of the alarms from naturally occurring radioactive materials. In 2005, CBP estimated more than 600,000 containers passed through the RPMs. The Standard Operating Procedures (SOP) for a radiation alarm require CBP officials to take the driver's license from the vehicle's driver and determine whether that individual is listed on any of the criminal databases. The SOPs also require the CBP officials to conduct a second check of the vehicle with a radiation isotope detector. Each step of the alarm resolution is accompanied by documentation, which is subsequently filed, and the alarm information is entered into a master spreadsheet.

---

[58] This data was supplied to the Subcommittee by CBP in March 2006.

[59] *See* GAO-06-389, "Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain," March 2006, pp. 16-17.

[60] *Ibid.*, p. 17.

[61] *Ibid.*, pp. 18-19.

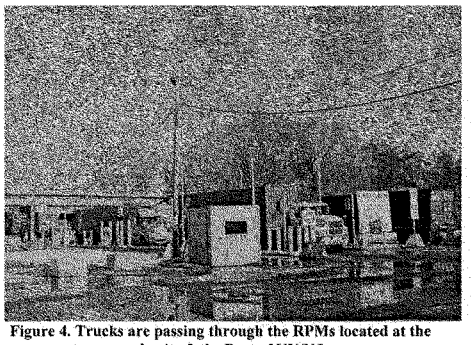


Figure 4. Trucks are passing through the RPMs located at the entrance and exit of the Port of NY/NJ.

During an inspection of the DNDO Countermeasures test bed at the Port of New York/New Jersey, PSI staff observed an alarm resolution in progress. In that episode, a truck had alarmed the RPM at the main entry and was then directed by the security guard to the secondary inspection area to await the arrival of CBP officers.[62] At the secondary inspection location, CBP officials conducted tests with a radiation isotope detector that was mounted to a Smart Cart. PSI staff rode in the Smart Cart as it drove around the truck, using the radiation equipment to scan the truck. (See Figure 5, below.) The results of the scan were available after

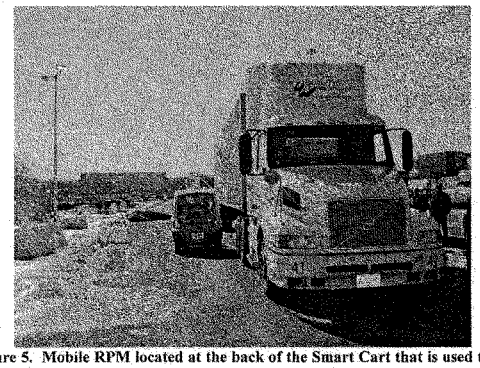


Figure 5. Mobile RPM located at the back of the Smart Cart that is used to determine the source of the radiation. After a truck alarms the RPM located at the entrance/exit to the Port, the truck is sent to the secondary inspection area.

approximately two minutes and identified the source as low levels of Cesium-137. Based on the manifest review, which identified the cargo as furniture with marble, and the radiation isotope information from the Smart Cart, CBP officers determined there was no need for a physical inspection and allowed the truck to proceed. Staff observed the CBP officers follow the appropriate procedures and protocols prior to releasing the container.

3. San Ysidro

The Port of San Ysidro in Southern California is the busiest port of entry into the United States for passenger vehicles and pedestrian traffic. With 24 vehicle lanes and 24-hour, seven-days-a-week operations, San Ysidro sees massive traffic, and in Fiscal Year 2005, processed almost 17 million passenger vehicles, more than 31 million passengers in vehicles, more than 100,000 buses, close to one million bus passengers, and more than 8.7 million pedestrians.

---

[62] Until the permanent booth to house CBP officers is built, CBP officers at this location are notified by the security guard and the truck is held at the secondary inspection area until arrival of the CBP officers.

There are RPMs deployed at each of the 24 lanes of traffic, as well as another RPM at the secondary location. According to senior CBP personnel, even though approximately 50,000 passenger vehicles are processed daily, they incur only 10-12 alarms. These alarms are easily resolved with the vehicles being screened again by an RPM at secondary and then scanned with a RIID in order to identify the particular isotope. Senior CBP personnel also stated that screening one hundred percent of the cars and buses with RPMs did not have a negative impact on the flow of traffic.

4. Recommendations

Effectively detecting and interdicting radiological or nuclear material is critical to U.S. homeland security efforts. As such, the Subcommittee staff makes the following recommendations:

- DNDO and CBP should accelerate the deployment of RPMs.
- DNDO should ensure that the NNSA's Megaports Initiative – which provides radiation detection to major foreign ports – is better coordinated with CSI.
- DNDO should continue testing new technology and endorse technologies equivalent to the Hong Kong screening concept, which is described in detail below.

F. Megaports Initiative

As part of the U.S. Government's layered strategy to secure the global supply chain and prevent nuclear or radiological smuggling, the Department of Energy (DOE) National Nuclear Security Administration (NNSA) program operates the Megaports Initiative. Under the auspices of this program, radiation detection equipment is provided to major international ports. This equipment is installed by the U.S. Government in coordination with the host government to screen all outbound containers regardless of destination (i.e. – containers destined for the United States as well as Asia are screened).

To date, Megaports equipment has been installed in five foreign ports: (1) Piraeus, Greece; (2) Rotterdam, Netherlands; (3) Colombo, Sri Lanka; (4) Algeciras, Spain; and (5) Freeport, Bahamas. The port of Antwerp, Belgium will be operational shortly as well. Nevertheless, progress in Megaports has been slow. NNSA plans to implement Megaports at up to 60 seaports, and given progress to date, this goal appears a bit ambitious. Concerns regarding the impact of Radiation Portal Monitors on commerce have prevented Megaports from quickly expanding. Additionally, the Megaports Initiative has increased its coordination with the Container Security Initiative, yet continues to operate as a separate and distinct program. Moreover, international agreements establishing either a CSI port or a Megaport are rarely negotiated together. This lack of coordination may contribute to an unnecessary expenditure of funds and resources.

1. Recommendations

Because the Megaports Initiative represents one aspect of the layered security strategy, and is the first line of defense, the Subcommittee staff makes the following recommendation:

- The U.S. Government must enhance the coordination between CSI and Megaports.

G. Private-Sector Screening

Continuing the partnership with the private sector is critical to effective screening. Since the announcement of the RPMP, CBP has worked with private companies – particularly, FEDEX and UPS – to encourage these companies to screen their packages. PSI staff applauds CBP's efforts to create this public-private partnership. As part of its oversight investigation, PSI assessed the screening operations at FEDEX's international hub at Charles De Gaulle Airport (CDG) in Paris. This hub is responsible for processing packages originating in the Middle East, Russia, and Northern Africa. FEDEX has implemented Radiation Portal Monitors to screen all shipments bound for the United States, regardless of whether those shipments are transiting the United States or if the United States is the final destination. While this operation is noteworthy and likely of great benefit, DHS has yet to validate the performance of these portals. To ensure that these RPMs are effective at screening for radiation and nuclear materials, staff recommends that DHS immediately commence an evaluation of these RPMs and the other RPMS deployed by FEDEX and UPS.

H. One Hundred Percent Screening of Containers

As discussed in detail above, ATS, the targeting system used to discern high-risk containers, is flawed. It is therefore crucial that U.S.-bound containers are screened effectively. The only effective screening mechanism employs both an x-ray and a radiation scan. Only the combination of those two scans can provide a reliable answer to the perplexing question of "what's in the box?" However, in Fiscal Year 2005, only 0.38 percent of containers were screened with a non-intrusive imaging device and only 2.8 percent of containers were screened for radiation prior to entering the United States.[63] Overall, CBP screens or physically examines only 5.4 percent of containers with an NII machine and less than 40 percent with RPMs. When combined with the problems in ATS, these facts expose serious vulnerabilities in our cargo screening processes.

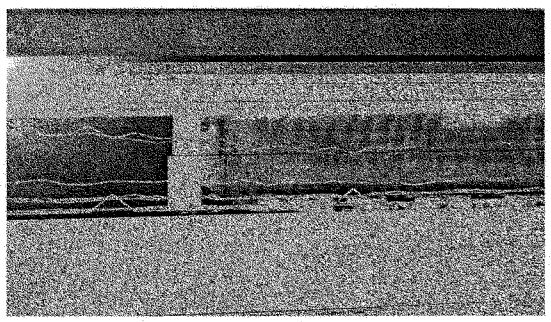


Figure 6. This ICIS image demonstrates the ability to view the RPM scan and x-ray simultaneously.

1. The Hong Kong Screening Concept [64]

While CBP screens a *de minimus* rate of containers, the private sector is developing systems that will screen every single container entering a port. A promising concept in Hong Kong -- the Integrated Container Inspection System (ICIS) -- demonstrates the potential to screen up to 100 percent of containers. At two gates in the Hong Kong International Terminals, each container entering the Hong Kong port is moved through an integrated system that features a non-intrusive image machine, a Radiation Portal Monitor, and an Optical Character Recognition System that identifies the container. Coupling these technologies allows for the most thorough scan currently available. Moreover, this scan does not impede the flow of commerce, and the equipment used is equivalent to or exceeds equipment currently used in the United States.

To ensure 100 percent screening, the system is deployed at the entry gate and at the dockside. Dockside screening ensures that transshipped containers, which are simply passing through the Hong Kong port, are also scanned. The image generated by this scan is stored electronically to be examined later. The scanning of all containers at the entry gate negates the burdensome and time consuming logistics of locating and retrieving each high-risk/suspect container from the copious stacks of containers. Rather, ICIS allows authorities to view the image immediately and then determine if an additional image or physical inspection is necessary to resolve an anomaly or alarm. If widely implemented, this system or equivalent technology may allow for 100 percent of all containers to be screened upon arrival at any port. In addition, this process would enable CBP to analyze a container in-transit and determine if an inspection is necessary upon arrival in the United States. Moreover, if an event does occur, this system would provide a forensics capability to investigate the incident.

---

[63] This data was supplied to the Subcommittee by CBP in March 2006.

[64] PSI staff is not endorsing ICIS, but rather recognizes this promising concept that demonstrates the ability to enhance our supply chain security by screening more containers with both non-intrusive equipment and radiation detection equipment.

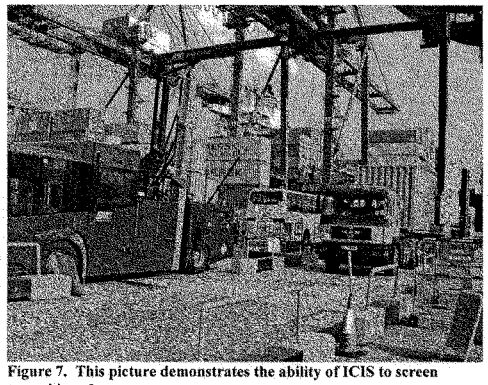


Figure 7. This picture demonstrates the ability of ICIS to screen transshipped cargo.

The Hong Kong Container Terminal Operators Association (HKCTOA) has asked DHS to evaluate the efficacy of the system as well as the potential of linking this concept to CSI. DHS responded to the HKCTOA request in November 2005, and signaled its interest in developing policies, procedures, and response protocols to integrate ICIS into its current security programs. HKCTOA provided data from its scans for further analysis, and DHS is presently studying the system. However, DHS is concerned about the efficacy of the technology, the effects on commerce requiring 100 percent screening, and more importantly, the changes ICIS makes to the "Customs to Customs" relationship between the United States and the CSI host government.

Possible benefits of the Hong Kong approach include the following:

- Negotiating directly with terminal operators to install a Hong Kong-type system would allow the U.S. Government to link together an RPM and VACIS scan. Such a combined scan would exceed current domestic or international scanning capabilities. Additionally, the foreign terminal operators own their ports and can direct the installation of RPMs. The Department of Energy Megaports program is being confronted with considerable resistance as it attempts to install RPMs at ports abroad. A program similar to ICIS could ameliorate this resistance and quickly enhance the security of the global supply chain.

- One hundred percent scanning does not require that all of the images be analyzed. This model would simply ensure that all high-risk containers are examined overseas and that the examination is recorded. The targeting model could still be utilized to pinpoint which containers would be further examined. Moreover, technology firms are developing technology that would automate the review of images, which may eventually allow for the review of all containers.

- ICIS or equivalent technology could contribute to the security of global trade if an event does occur because the infrastructure would already be in place to screen 100 percent of containers at major ports. Additionally, it would allow for post-event analysis if an event did occur, similar to the process used following the London bombings in July 2005. ICIS could also help the intelligence community track proliferation and uncover global smuggling networks.

- The implementation of ICIS or similar technology could yield significant cost savings to CBP because the majority of targeting and analysis of images could occur remotely, thus reducing the substantial costs of stationing CBP personnel abroad under the CSI program.

- If foreign terminals decided to purchase ICIS or equivalent technology, it could be implemented quickly and potentially cover upwards of 80 percent of global trade, since the majority of foreign terminals are privately owned.

2. One Hundred Percent Screening in Russia

In July 2005, PSI staff observed examples of 100 percent screening for radiation when conducting oversight over the Second Line of Defense program in Russia.

(a) St. Petersburg Seaport

The St. Petersburg Seaport is part of the Megaports Initiative, the program designed to provide RPMs to foreign seaports to ensure that they screen cargo for radiation. Similar to other global ports, this port is rapidly expanding and anticipates moving upwards of one million 20-foot equivalent units (TEU) in 2005.[65] Much of the container traffic from St. Petersburg is shipped to European Union ports, with the largest percentage going to the Port of Rotterdam. According to Russian Customs, all incoming and outbound containers and people are inspected for radiation. Russian Customs permanently stores information on positive alarms, and 59 RPMs are deployed throughout the seaport. These alarms are configured with an assortment of video cameras to record any positive hits for radiation. Russian Customs uses a matrix to assist in alarm resolution and receives between 10-12 alarms per day. Following a positive hit, the suspect container is directed towards secondary inspection. Most positive alarms are resolved within 30 to 40 minutes. Within Russian Customs, a specialized service – TKDRM – was created in 1995 to focus on radiation and nuclear issues. Throughout Customs, there are close to 700 people in this service with eight TKDRM personnel located at the Port of St. Petersburg.

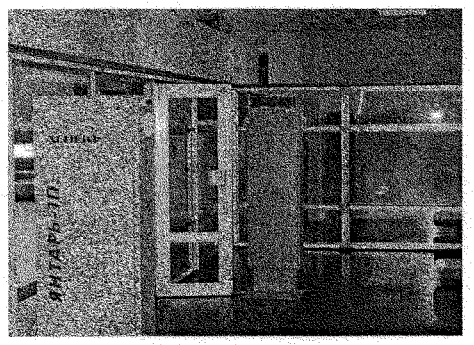


Figure 8. RPMs in Russia to screen air passengers and baggage.

(b) Pulkova Airport in St. Petersburg

Pulkova Airport is part of the Second Line of Defense (SLD) program, which provides radiation detection equipment to Russia to interdict nuclear/radiological smuggling attempts. At Pulkova Airport, every perimeter is covered with RPMs, and all cargo, people, cars, and employees are screened for radiation. Eighty-nine positive hits were recorded in July, and each was resolved. According to Russian Customs, this extensive screening apparatus does not hinder the flow of commerce. Moreover, nuclear/radiation screening is mandated by the Russian government and concerns regarding hindering the flow of commerce are not of primary concern. DHL, UPS, and FEDEX operate out of St. Petersburg Airport, where each company's respective cargo is screened with both non-intrusive imaging equipment and a RPM. This includes cargo on passenger jets. In addition, all general aviation cargo and baggage is screened as well as cargo and baggage for official delegations. The RPM equipment at Pulkova was installed within 18 months of the first planning meeting. One hundred percent screening is now a reality at the Pulkova Airport and Subcommittee staff urges DNDO to assess this effort and glean lessons for U.S. detection.

---

[65] A TEU is a measurement of the containerized cargo capacity of a shipping container.

(c) Sheremeteyevo International Airport in Moscow

Sheremeteyevo is Russia's largest airport and is part of the SLD program. There are 100 RPMs deployed throughout the airport to screen all incoming and outgoing baggage, people, cargo, and employees for radiation. Thirty-four of the RPMs were purchased by SLD and the remainder by Russia. Russian Customs selectively x-rays cargo based on risk delineated by countries of interest and other manifest information of concern. There are 12 trained nuclear experts, all part of TKRDM, who handle nuclear and radiological associated issues at Sheremeteyevo. The airport receives between 15 and 20 positive hits per day. Russian Customs electronically stores information on such positive alarms for six months and keeps a paper record of such alarms for several years. Furthermore, when an individual sets off an alarm and asserts that he or she is undergoing radiological medical treatment, Russian Customs conduct tests to ensure that they are not using medical treatment as an excuse for smuggling nuclear/radiological material.

(d) Verification of Radioactive Shipments

Russian Customs verifies the contents of all declared radioactive shipments with a handheld detector. This verification system was implemented after Russians Customs discovered unauthorized material had been smuggled within a declared radioactive shipment. The verification procedures include (1) weighing the package; (2) x-raying the package (to look for any additional shielding); and (3) checking the declared shipments with a germanium handheld detector to validate the isotope. The entire process takes a maximum of five minutes. Staff recommends that DNDO consider implementing a similar process to assess domestic shipments of radioactive material.

V. OTHER PROMISING TECHNOLOGY

"They're as dumb as a fence post, so we just want to make them smarter."

- Former CBP Commissioner Robert Bonner

Former Commissioner Bonner accurately described shipping containers and the difficulty in trying to secure these containers. As discussed earlier, securing the supply chain is made more difficult by the fact that, as a container moves from point to point, many different companies have to coordinate their activities in the supply chain. Each point represents a potential vulnerability; yet, new technology is being developed to close those vulnerabilities.

This new technology may enable companies to track a container remotely and ascertain if that container had been opened at any point during transit. Additionally, this technology may deter theft and ensure that the containers arrive in a timely manner. Private industry has developed electronic seals that communicate with active radio frequency identification technology as a way to secure and track the container.

Container Security Devices (CSD), coupled with radio frequency identification devices (RFID), have demonstrated the potential to detect whether a container door is opened without authorization, as well as any changes in light and temperature. Once a container has been breached, the RFID will send that information to a central monitoring system, thereby signaling that the container has been compromised. To accelerate the development of this technology, CBP operates the Smart Box program to enhance the security of oceangoing containers. The Smart Box program is designed to identify technologies and systems to provide a more secure shipping container with the ability to minimize the potential of insertion of lethal cargo, as well as to generate advance notification of any unauthorized opening of the containers and the presence of lethal cargo.

CBP is also actively engaged in the evaluation of technology designed to incorporate additional sensing capabilities with the goal of providing six-sided container security (*i.e.* all sides of a container), or an Advanced Container Security Device (ACSD). CBP may require that shippers or participants in C-TPAT utilize a RFID or a CSD.

VI. OTHER SECURITY RISKS

A. Trash Poses Unique Supply Chain Security Problems

A special security risk involves the importation into the United States of containers carrying trash. Trash containers pose inherent difficulties in terms of supply chain security, because tracing the supply chain for trash cargos with any certainty is difficult. Many different individuals and entities create trash and contribute to trash collections, with virtually no security measures in place to screen specific trash contributions or preclude illegal materials. This process makes it logistically burdensome, if not prohibitively expensive, for even a trash importer with the best intentions to understand and monitor what is being transported in particular trash containers each day. Other cargos may be equally as dense as trash, but importers often have better control over the specific content and origin of the supply. With other cargos, it is often possible to trace the origin, mid-course and ending point of the journey of the cargo, and take steps to monitor and ensure the security of the supply chain. Until a similar system is established for the supply chain of trash importers, DHS must take additional security precautions before allowing trash containers to enter the United States.

Since 1998, the greater Toronto, Canada, area has shipped hundreds of thousands of containers carrying trash or municipal solid waste (MSW) across U.S. borders.[66] According to the Department of Homeland Security (DHS) Inspector General's office, in 2004 alone, Canada shipped approximately 100,000 containers of trash across U.S. borders into Michigan, an eight percent increase over 2003.[67] Another 10,000 containers of MSW comes through nine other ports of entry on both the Northern and Southern borders.[68]

Over the past few years, there have been numerous incidents where Canadian trash containers have brought more than just trash into the United States. For example:

- In April 2003, police in Sumpter Township, Michigan, found 50 pounds of marijuana in a Canadian trash truck.
- In August 2003, a Canadian trailer carrying a trash container was pulled over for being overweight. The policeman on duty, after obtaining consent from the driver and passengers, found a blue duffel bag containing $539,200.
- On September 24, 2003, Customs and Border Protection (CBP) agents apprehended a trash truck driver for attempting to enter the United States with one ton of marijuana. The approximately 2,000 pounds of illegal drugs were packed into 59 plastic bags and hockey equipment duffel bags and constituted one of the biggest drug busts in recent Michigan history. Law enforcement officials valued the drug's street value at approximately $9 million.
- In October 2002, a trash truck was leaking blood from its trailer as it crossed the Ambassador Bridge from Canada into the United States. As the truck was unloaded at a Waste Management Recovery station in Detroit, it became clear that medical waste was a large percentage of the waste in the trailer.
- The DHS Inspector General has found that from 2003 to 2004 medical waste, illegal drugs, and illegal currency have been transported into the United States in trash containers.[69]

The following photograph of an x-ray image of a container carrying Canadian trash, taken at a Michigan border crossing, illustrates the problem. (See Figure 12) Even with an x-ray image, it is impossible to see the contents of the container because the trash is so dense that the x-ray cannot penetrate it. The inability to see what is inside the container endangers national

---

[66] *See* "Audit of Screening Trucks Carrying Canadian Municipal Solid Waste," U.S. Department of Homeland Security, Office of Inspector General, January 2006 [One page unclassified summary.]

[67] *Ibid.*

[68] *Ibid.*

[69] *Ibid.*

security, because weapons or nuclear material could be concealed and CBP border personnel would have no effective method of detection, short of physically inspecting each and every shipment, which is beyond current resources. It is also inherently difficult and dangerous to physically inspect trash containers.

Figure 9: X-ray image of a Container Full of Trash

1. Cost-Benefit Analysis Weighs Against Trash Imports

The Subcommittee understands that other materials, such as concrete or bricks, pose similar security challenges in terms of being as dense as trash when screened with NII or RPMs. A cost-benefit analysis of these imports, however, would likely show that products like concrete or bricks contribute positively to the U.S. economy because their introduction into the flow of commerce provides building materials, contributes to reasonable construction costs, and helps create new jobs. Such materials also pose lower security risks, since, unlike trash, their supply chains can be more easily monitored and made secure. In contrast, if CBP were to conduct a cost-benefit analysis of trash imports, the analysis would likely show that the security risk of trash containers to the country and the costs associated with reducing that risk far outweigh any economic benefit.

2. DHS Inspector General Report

Two years ago, the security problems associated with trash containers crossing U.S. borders without effective screening technology led Senator Levin, Senator Stabenow, and Congressman Dingell to ask the DHS Inspector General's office to review the effectiveness of CBP's screening methods. The Inspector General's disturbing report, released in January of this year, in unclassified and "official use only" versions, identifies flaws and vulnerabilities associated with current methods to screen containers entering the United States.

The DHS Inspector General noted that every passenger vehicle and truck entering the United States at the Detroit and Port Huron ports of entry pass through RPMs and some trucks receive an x-ray screening.[70] However, as noted above, trucks carrying trash containers cannot be effectively screened with either the RPM or the x-ray technology. After a thorough evaluation of the ports of Detroit and Port Huron, Michigan, the DHS Inspector General found:

- Improvements are needed in the inspection process.
- The ports vary in how they select and inspect cargo and conduct x-ray exams.
- There is no Centralized Exam Station in Michigan.
- The Commissioner of the CBP should conduct a risk analysis and develop minimum requirements for selecting and inspecting trucks carrying Canadian trash.

The "official use only" version of the Inspector General's report describes in greater detail the security risks associated with trash containers entering the United States under the

---

[70] *Ibid.*

present circumstances. However, until this version of the report is released to the public, the nature of the security concerns identified by DHS cannot be described in specific terms.

3. Recommendations

The Subcommittee staff makes the following recommendations:

- Until CBP can ensure that the supply chain of a trash importer is secure or develops protocols ensuring adequate inspection of individual trash containers, CBP should not allow trash containers to enter the United States.
- At a minimum, DHS should immediately adopt the Inspector General's recommendation to conduct a risk analysis and develop minimum requirements for selecting and inspecting trucks carrying Canadian trash. Until these steps are taken, CBP should place a moratorium on allowing trash containers into the United States.
- Congress should enact into law the provisions recently adopted by the U.S. Senate to impose a fee on international shipments of trash to pay for a more rigorous inspection regime to protect U.S. citizens from the security risks currently associated with trash containers.

VII. CONCLUSION

In the four years following the September 11th attacks, America has made significant progress in securing the global supply chain. Under the CSI program, CBP officers are now stationed in numerous foreign ports to facilitate the inspection of high-risk containers before they arrive at U.S. ports. More than 700 Radiation Portal Monitors have been deployed in ports all over the world. CBP, through the C-TPAT program, is developing significant ties with private-sector entities to enhance security of the global supply chain.

Despite these gains, much more work needs to be done. ATS, the system used to target high-risk containers, has certain significant flaws, such as its dependence on unreliable information. Moreover, although the central purpose of CSI is to inspect high-risk containers before they arrive at U.S. ports, many such containers pass through CSI ports without any inspection. To make matters worse, CBP cannot demonstrate that those targeted containers are inspected upon their arrival in the United States. The deployment of radiation detection equipment has been woefully inadequate. America must enhance these programs to secure the global supply chain or we remain vulnerable to the Trojan Horse attack – in which terrorists or WMD are smuggled into our ports.

To strengthen our defenses and prevent such attacks, PSI recommends the following:

A. Container Security Initiative

- The use of a specialized subset of ATS, such as in Rotterdam, must be expanded to other CSI ports.
- The targeting system – ATS – must be adjusted to effectively identify high-risk containers.
- The number of inspections conducted abroad needs to increase dramatically.
- The arbitrary distinction between high-risk cargo due to narcotic smuggling and high-risk cargo due to terrorism is difficult to identify and may demonstrate a potential vulnerability.
- The Virtual CSI program is an innovative concept that must be expanded, especially if coupled with the Hong Kong Screening Model or equivalent technology, which is discussed below.
- The CSI program should focus on improving inspection rates at existing CSI ports, prior to expanding to other ports.
- CSI targeting can be conducted domestically. CBP should readjust its staffing model and utilize a combination of officers in-country and at the NTC.
- Standards for inspections and technology must be incorporated into the DOPs signed by the United States and host governments to establish a CSI Port.

B. Customs-Trade Partnership Against Terrorism

- The validation process needs to be strengthened to include a review of additional supply chains.
- A revalidation strategy must be developed and validations must be conducted for each C-TPAT member with a clear strategy and timeline for completing the validations.
- CBP should work collaboratively with C-TPAT members to develop self-policing standards.

C. Automated Targeting System

- ATS must be validated and proven to accurately identify high-risk containers.
- ATS should incorporate additional data elements to enhance its targeting ability including entry data.
- CBP should develop procedures to facilitate the filing of entry data prior to the arrival of the vessel at a U.S. port.
- CBP should establish baseline performance measures to evaluate the effectiveness of ATS as a targeting system.
- ATS rules need to be flexible and take into account findings from other high-risk cargo examinations and intelligence, as well as local factors.
- Simulated and red-team testing must be conducted on ATS.

D. The Radiation Portal Monitor Program

- DNDO and CBP should accelerate the deployment of RPMs.
- DNDO should ensure that the NNSA's Megaports Initiative – which provides radiation detection to major foreign ports – is more closely linked, with CSI.
- DNDO should continue testing new technology and endorse technologies equivalent to the Hong Kong screening concept, which is described in detail below.

E. The Megaports Initiative

- The U.S. Government must enhance the coordination between CSI and Megaports.

F. Other Security Risks

- Until CBP can ensure that the supply chain of a trash importer is secure or develops protocols ensuring adequate inspection of individual trash containers, CBP should not allow trash containers to enter the United States.
- At a minimum, DHS should immediately adopt the Inspector General's recommendation to conduct a risk analysis and develop minimum requirements for selecting and inspecting trucks carrying Canadian trash. Until these steps are taken, CBP should place a moratorium on allowing trash containers into the United States.
- Congress should enact into law the provisions recently adopted by the U.S. Senate to impose a fee on international shipments of trash to pay for a more rigorous inspection regime to protect U.S. citizens from the security risks currently associated with trash containers.

♦ ♦ ♦

APPENDIX A

Chairman's Letters From the Senate Permanent Subcommittee on Investigations

February 1, 2005:	**Letter to Under Secretary for Border and Transportation Security Asa Hutchinson**[71]
October 7, 2005:	**Letter to Department of Homeland Security Secretary Michael Chertoff**
December 20, 2005:	**Letter to Department of Homeland Security Secretary Michael Chertoff**
February 3, 2006:	**Letter to National Nuclear Security Administration Ambassador Linton Brooks**
February 3, 2006:	**Letter to Acting Customs and Border Protection Commissioner Deb Spero**
February 3, 2006:	**Letter to Domestic Nuclear Detection Office Director Vayl Oxford**

[71] A copy of this letter was also sent to then-CBP Commissioner Robert Bonner.

United States Senate
COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

February 1, 2005

VIA U.S. MAIL & FACSIMILE (202/282-8407)

The Honorable Asa Hutchinson
Under Secretary for Border and Transportation Security
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Hutchinson:

In light of the September 11, 2001, terrorist attacks, concern has increased that terrorists could smuggle weapons of mass destruction ("WMD"), or their components and other potentially lethal devices, in the approximately 9.7 million ocean going containers that arrive in the United States every year. As part of its overall response to the threat of terrorism, the Department of Homeland Security's Bureau of Customs and Border Protection ("Customs") began to deploy sophisticated technology called radiation portal monitors ("RPMs") at some of our ports of entry. These RPMs are designed to detect radiological devices and nuclear weapons. Installing such equipment at our borders is a critical component in reducing the Nation's vulnerability to terrorism.

Recent studies indicate that a nuclear or radiological event at a U.S. port could inflict numerous casualties as well as result in an economic impact of greater than one trillion dollars to the U.S. economy. Given the enormous stakes involved in the federal government's response to nuclear terrorism, members of the House and Senate in a bicameral and bipartisan fashion have collaborated to review the actions taken by DHS and Customs to safeguard our country from a nuclear attack.

As you know, the deployment of RPMs began in October 2002. Customs asserted that the critical first 3 phases of the deployment (i.e. international mail and consignment courier facilities, northern border crossings, and 22 major ports) would be completed by March 2005. As you know, the proposed project schedule will not be met.

On January 18, 2005, Congressional staff met with Customs to discuss a number of outstanding issues related to the deployment of RPMs. While there was productive dialog, many of the questions and concerns posed by staff remain unanswered. These concerns are similar to those raised by a host of major audits conducted by both the Government Accountability Office and the Office of Inspector General for the Department of Homeland Security regarding these very efforts. While we continue to support this important program in concept (and are prepared to offer all appropriate support), it remains imperative that the key deficiencies associated with this effort be expeditiously addressed.

In order for us to fully assess the adequacy and pace of the deployment of the RPMs, please provide the Subcommittee and the Committees listed below with the following no later than February 15, 2005:

1. Copies of all Project Execution Plans ("PEP") for the deployment of RPMs, including all drafts of such a report.

2. A copy of the final report on energy windowing, including all drafts of such a report.

3. An inventory and description of all non-intrusive devices utilized by Customs to screen cargo containers imported into the United States.

4. All standard operating procedures related to the utilization of non-intrusive technology to screen imported cargo containers.

5. The number of cargo containers annually imported into the United States. Please provide the total number of imported containers and delineate the number of imported containers by the mode of transportation (i.e. rail, sea, land).

6. The number of imported cargo containers annually inspected by Customs.

7. All documents relating to "red team" exercises utilized to test the inspections of cargo containers imported into the United States.

Please produce copies of the documents and other information responsive to the above requests to each individual listed below. Due to new security procedures, it is necessary to make advance arrangement for the delivery of the documents through courier or messenger service. Please contact the following individuals in order to obtain the procedures necessary to deliver the documents to each requester: Raymond V. Shepherd III, Staff Director and Chief Counsel to the Permanent Subcommittee on Investigations ("Subcommittee"), (202) 224-3721; Laura Stuber, Minority Counsel to the Subcommittee, (202) 224-9505; Lesley Leger-Kelley, Senior Counsel to the Committee on Homeland Security and Governmental Affairs ("Committee"), (202) 224-4751; Jason Yanussi, Minority Professional Staff Member to the Committee, (202) 224-2630; Chris Knauer, Minority Investigator to the U.S. House Energy and Commerce Committee, (202) 226-3400; and Eric Edwards, Legislative Director for Congresswoman Jane Harman, (202) 225-8220.

Thank you in advance for your prompt attention to this matter.

Sincerely,

NORM COLEMAN
Chairman
Permanent Subcommittee on Investigations
U. S. Senate

CARL LEVIN
Ranking Minority Member
Permanent Subcommittee on Investigations
U. S. Senate

SUSAN M. COLLINS
Chairman
Committee on Homeland Security
and Governmental Affairs
U. S. Senate

JOSEPH LIEBERMAN
Ranking Minority Member
Committee on Homeland Security
and Governmental Affairs
U. S. Senate

JOHN D. DINGELL
Ranking Minority Member
Committee on Energy and Commerce
U. S. House of Representatives

JANE HARMAN
Ranking Minority Member
Select Committee on Intelligence
U. S. House of Representatives

cc: The Honorable Robert C. Bonner
Commissioner
Customs and Border Protection
U. S. Department of Homeland Security

Congress of the United States

Washington, DC 20510

October 7, 2005

The Honorable Michael Chertoff
Secretary
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Chertoff:

Over the past several years, our respective Committees have examined the methods used by Customs and Border Protection (CBP) to target and subsequently search U.S.- bound, high-risk shipping containers for weapons of mass destruction (WMD), counterfeit goods, stowaways, and other forms of contraband. In addition to being used for common smuggling purposes, it is generally recognized that seagoing containers could be used to deliver a WMD to a U.S. port or city. The primary tool utilized by CBP to attempt to identify high-risk containers destined for the U.S. and target them for further examination is the Automated Targeting System (ATS).

ATS is a collection of rules that allows inspectors to target inbound containers based upon manifest information, entry data, intelligence, and other information. Inspectors using ATS are, in theory, able to rank containers by risk, then conduct further analysis to determine whether a suspect container should be inspected -- either physically or by non-intrusive imaging -- before the shipment is granted U.S. entry. As noted by CBP's Web site:

> "ATS . . . is a system that [assists CBP] officers in identifying imports which pose a high risk of containing narcotics or other contraband . . . The system standardizes bill-of-lading, entry, and entry summary data received from the Automated Commercial System (ACS) and creates integrated records called "shipments". These shipments are then evaluated and scored by ATS, through the use of over 300 weighted rules derived from targeting methods used by experienced [CBP] personnel. The higher the score, the more the shipment warrants attention."

While we agree that ATS has value in assisting "[CBP] officers in identifying imports which pose a high risk of containing narcotics or contraband," we continue to question both the degree to which this system is capable of accomplishing that task and the extent to which ATS is increasingly relied upon as the primary tool for determining which containers should receive an inspection.

Throughout many foreign ports where CBP has instituted the Container Security Initiative (CSI) program, staff have observed that CBP inspectors primarily, and sometimes exclusively, rely on the initial risk scores generated by ATS to determine which containers should be referred to their foreign counterparts for physical examination. It remains unclear to us whether a high ATS score realistically correlates to a finding that a container contains smuggled goods. For any evaluation of ATS, there are a number of other key issues that should be addressed. For example, do containers categorized as "high risk" by ATS carry more contraband (and thus possibly a WMD) than randomly selected containers? Does CBP have evidence that statistically validates that claim? Further, does CBP agree that the general category of contraband, whether stowaways, drugs, undeclared, or counterfeit drugs, serves as a surrogate for WMD for purposes of evaluating this program? If not, what variables would CBP use in this regard?

In March of 2004, the Government Accountability Office (GAO) provided testimony regarding their concerns about this system and noted the following:

> "Regarding recognized modeling practices, [CBP] has not subjected [ATS] to adequate external peer review or testing. It has also not fully implemented a process to randomly examine containers in order to test the targeting strategy. Without incorporating all key elements of a risk management framework and recognized modeling practices, CBP cannot be reasonably sure that its targeting strategy provides the best method to protect against weapons of mass destruction entering the United States and its seaports. (See GAO-04-557T "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection, March 31, 2004.")

On repeated occasions, staff has queried CBP officials regarding ATS, particularly to determine which shipments should be examined for potential WMD. We continue to question both the veracity of the testing and whether or not ATS has received any validation from a competent and objective authority. Moreover, we remain concerned that CBP will continue to rely on ATS as the primary tool for keeping dangerous goods -- including a WMD -- from entering the United States, without some indication that ATS does significantly assist CBP as a tested and validated risk management tool.

Given CBP's reliance on ATS, particularly as it rapidly expands its CSI program to more than 50 ports worldwide, we believe that it is imperative that this tool be vigorously peer reviewed and its effectiveness for managing risk be fully measured and documented. We also believe that this validation should be done by an objective third party entity. It is concerning that DHS cannot document or demonstrate any objective assessment of the system's capabilities and inherent limitations. Due to these issues, we are requesting the following by November 1, 2005:

1. Please convene an independent, outside panel to fully evaluate and peer review the capabilities of the ATS system in identifying risk related to inbound shipping containers, as well as any of its limitations as a risk management tool. This assessment should include a review of both the rules that are used to construct ATS scores, their reasonableness, their respective weighted scores, as well as the information and data utilized to generate these scores. The assessment should also measure whether increasing risk statistically correlates with actual discovered contraband. Our respective Committees are aware of the April 2005 Mitretek study involving ATS. While we applaud this as a first step in gathering key information about this system, we do not believe that this meets the intent of this request, particularly as it does not measure or validate ATS's effectiveness.

2. Please provide any studies, reviews, or analysis conducted by DHS, CBP, or any of its agencies that assessed or measured the capability of the ATS system. As the ATS score is perhaps the most relied upon method for determining which containers should be examined, please also include any analysis that is being used to set the degree to which CBP uses ATS as a risk management tool.

3. Please provide the information provided to CBP inspectors domestically and abroad on the ATS system and operating procedures for determining which inbound containers require an inspection.

We greatly appreciate your attention to this important homeland security issue. If you have any questions regarding the matters we have raised, please contact us or have your staff contact Christopher Knauer, Minority Investigator, U.S. House of Representatives Committee on Energy and Commerce at (202) 226-3400; Brian White, Professional Staff, U.S. Senate Permanent Subcommittee on Investigations, at (202) 224-3721; Kathleen Kraninger, Professional Staff, U.S. Senate Committee on Homeland Security and Governmental Affairs, at (202) 224-2186; Laura Stuber, Minority Counsel, U.S. Senate Permanent Subcommittee on Investigations, at (202) 224-9579; and, Jason Yanussi, Minority Professional staff, U.S. Senate Committee on Homeland Security and Governmental Affairs, at (202) 224-2630.

Thank you in advance for your prompt attention to this matter and for your continuing efforts on homeland security.

Sincerely,

Norm Coleman
Chairman
Permanent Subcommittee on Investigations
U.S. Senate

John Dingell
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives

Susan M. Collins
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

Carl Levin
Ranking Minority Member
Permanent Subcommittee on Investigations
U.S. Senate

Joe Lieberman
Ranking Minority Member
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

cc: Mr. Richard Skinner, Acting Inspector General
Department of Homeland Security

The Honorable David M. Walker, Comptroller General
Government Accountability Office

The Honorable Robert C. Bonner, Commissioner
United States Customs Service

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

December 20, 2005

VIA U.S. MAIL & FACSIMILE (202/772-9734)

The Honorable Michael Chertoff
Secretary
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Chertoff:

I traveled to Hong Kong last week and had the opportunity to meet with the Container Security Initiative (CSI) team as well as representatives of Hong Kong Customs at the Port of Hong Kong. Throughout the visit, I was happy to observe a close level of cooperation between Department of Homeland Security and Hong Kong Customs personnel, as well as the professionalism amongst the CSI team. I was also pleased to see that the Bureau of Customs and Border Protection (CBP) has implemented many of the recommendations from the Permanent Subcommittee on Investigations and Government Accountability Office (GAO) reports. While our oversight will continue, the progress in both CSI and the Customs-Trade Partnership Against Terrorism (C-TPAT) deserves immediate recognition. I look forward to continuing to work collaboratively with you to ensure that these programs complete the transition from promising concepts into sustainable security programs.

During this trip, I also toured the Port of Hong Kong and discussed security with representatives of Hutchinson Port Holdings (HPH). As the largest terminal operator in the world, HPH has an inherent interest in securing containers. To facilitate container security, HPH has worked with a technology vendor to develop a remarkable security system, the Integrated Container Inspection System (ICIS) that is capable of screening cargo containers upon entry to the port or prior to transshipment without impeding the flow of commerce or operations of the port. This system enables each container to move through an integrated system featuring a non-intrusive image machine (VACIS), a Radiation Portal Monitor (RPM), and an Optical Character Recognition System (OCR) to identify the container. Moreover, the equipment utilized in this system is equivalent to or exceeds equipment currently used domestically. In essence, HPH has demonstrated that one hundred percent screening can become a reality.

Although operational protocols and processes need to be developed, I hope to see the Department embrace this private sector initiative. It is important to note that this system is being embraced by importers, freight forwarders, and shipping lines as a tool to enhance security. Adding another layer of protection to supply chain security will enhance our collective homeland security.

The initial supply chain security programs developed after September 11th, especially C-TPAT, exemplified true public – private partnerships. In addition, C-TPAT embedded the notion of supply chain security in the private sector. While C-TPAT continues to grow and mature, it is critical that DHS continue to work with the private sector and promote innovative security concepts. Securing the supply chain is the foundation of international trade – and it is important that DHS continue to make progress to ensure global trade is truly secure. I believe the system I observed in Hong Kong could advance supply chain security and demonstrate yet another important public – private partnership.

In view of the work of my Subcommittee on supply chain security and my recent visit to Hong Kong, please provide the DHS assessment of this system as well as a plan to integrate ICIS into current security programs to the Subcommittee by January 15, 2005. I look forward to continuing to work this issue with you and your staff. If you or your staff has any questions, please feel free to contact Brian White, Professional Staff, at 202 – 224-3721.

Sincerely,

Norm Coleman
Chairman
Permanent Subcommittee on Investigations
United States Senate

NC:bw
cc: Ambassador Linton Brooks, Administrator, National Nuclear Security Administration
Ms. Deborah Spero, Acting Commissioner, U.S. Customs and Border Protection
Vayl Oxford, Director, Domestic Nuclear Detection Office
The Honorable Susan Collins, Chairman, U.S. Senate Committee on Homeland Security & Governmental Affairs
The Honorable Joseph Lieberman, Ranking Member, U.S. Senate Committee on Homeland Security & Governmental Affairs
The Honorable Peter King, Chairman, U.S. House of Representatives Committee on Homeland Security
The Honorable Bennie Thompson, Ranking Member, U.S. House of Representatives Committee on Homeland Security
The Honorable John Dingell, Ranking Member, U.S. House of Representatives Committee on Energy & Commerce
Mr. John Meridith, Managing Director, Hutchinson Port Holdings

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

February 3, 2006

VIA U.S. MAIL & FACSIMILE (202/586-3929)

Ambassador Linton F. Brooks
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Department of Energy
Forrestal Building, Room 7A199
1000 Independence Avenue, S.W.
Washington, D.C. 20585

Dear Ambassador Brooks:

Securing the homeland from Weapons of Mass Destruction (WMD) should be one of our top national priorities. Accordingly, our Subcommittee has closely followed the implementation of programs to confront this threat. In preparation for oversight hearings scheduled March 28th and 30th to examine efforts to detect and interdict a radiological or nuclear weapon, please provide the following no later than February 15, 2006:

1. The National Nuclear Security Administration (NNSA) Second Line of Defense (SLD) Strategic Plan inclusive of the Core program and the Megaports Initiative.

2. A list of all current and planned deployments of Radiation Portal Monitors (RPMs) outside of the U.S., as well as the number and type of RPMs deployed at each location in support of the SLD program. Please identify the number of RPMs funded by the United States versus the host government.

3. The NNSA position regarding the Hong Kong screening concept which is commonly referred to as the "Integrated Container Inspection System."

4. A list of all training provided by NNSA to state or local agencies in the detection of radioactive materials. Please specify who conducted the training, the purpose of the training, the type, and length of training as well as materials provided to the state or local agencies.

5. The three studies as referenced in the GAO reports, that were commissioned to better understand the unique challenges confronting the SLD program.

6. Answers to the following questions or requests for information with respect to the SLD programs:

    a. What percentage of maritime containers entering the United States are screened for radiation?

b. How many positive alarms for radiation have been recorded by RPMs deployed abroad? Of these alarms, how many are nuisance alarms? How many alarms have recorded threat materials?

c. Why are gamma only RPMs utilized at SLD sites? Please provide the plan for updating these RPMs as appropriate.

d. Has any red teaming occurred to test currently deployed RPMs? If so, please provide the results and testing protocol.

e. How many personnel have been trained to use the RPMs? Please indicate the number of available and trained personnel at each deployment site.

f. A summary of the RPM maintenance and calibration schedule.

g. Which border sites are currently linked to national and regional command centers?

h. DOD has plans to implement an Employee Dependability Program in Uzbekistan, that includes background checks, urinalysis, and sensitivity training to combat some of the underlying employee-related issues. The Russian government has requested that DOE implement a similar type of program. What steps have been taken to develop this type of program? Is there an implementation schedule? If so, please provide.

i. What sites under the SLD-Core program have received anti-corruption training?

j. Are there any instances in which an employee at a RPM deployment site was discovered to have been compromised? If so, please provide the number of instances and identify the locations where the compromise occurred.

k. Please provide the country-wide corruption assessments conducted by DOE employees in prioritizing countries to be included in the SLD-Core program.

l. Please provide the standard operating procedures for resolving positive alarms.

m. Under the Megaports Initiative, the NNSA installs and provides radiation detection equipment to countries that sign agreements with the United States. Please provide copies of all signed agreements.

n. With regards to the equipment currently deployed to Belarus and Turkey as referenced in the GAO reports, what efforts are being made to ensure that the equipment is being properly maintained?

o. What is the status of the new implementing agreements to be signed between DOE and the countries with previously installed non-DOE equipment?

p. In fiscal year 2005, DOE assessed each location where gamma-only portal monitors were being maintained. Please provide a summary of the assessment conducted for each location and the prioritized list of which sites should receive upgraded equipment.

q. Please provide a list of locations where technical resources have been provided under the Megaports Initiative to complement the Container Security Initiative.

r. What form of information sharing has been conducted between the NNSA and host countries? Has this practice of information sharing been formalized into a written agreement? If so, please provide copies of all such documents.

s. What is the role of the Domestic Nuclear Detection Office (DNDO) in the programs and efforts to install and provide radiation detection equipment abroad?

t. Describe the relationship between the NNSA and the DNDO.

u. What is the plan for increasing participation by host countries and decreasing the reliance on U.S. government equipment and funds?

Thank you in advance for your continued cooperation with our oversight investigation. We look forward to working with you to strengthen this vital program. If you or your staff has any questions regarding this matter, please contact us or have your staff contact Brian White, Professional Staff, with the Senate Permanent Subcommittee on Investigations, at (202) 224-3721 or Madelyn Creedon, Professional Staff, with the Senate Armed Services Committee, at (202) 224-3871.

Due to new security procedures, it is necessary to make advance arrangement for the delivery of documents through courier or messenger service. Please contact the aforementioned staff in order to obtain the procedures necessary for delivery.

Sincerely,

Norm Coleman
Chairman
Permanent Subcommittee on Investigations

Carl Levin
Ranking Minority Member
Permanent Subcommittee on Investigations

cc: The Honorable Michael Chertoff, Secretary, U.S. Department of Homeland Security
The Honorable David Walker, Comptroller General, U.S. Government Accountability Office

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

February 3, 2006

VIA U.S. MAIL & FACSIMILE (202/344-2152)

Ms. Deb Spero
Acting Commissioner
U.S. Customs and Border Protection
Department of Homeland Security
Washington, DC 20229

Dear Acting Commissioner Spero:

Securing the homeland from Weapons of Mass Destruction should be one of our top national priorities, and as such, our Subcommittee has closely followed the implementation of programs to confront this threat. Our oversight hearing, "The Container Security Initiative and Customs-Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?" on May 26, 2005, highlighted several areas of concern with these programs. Since then, we have noted the improvements in the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) initiatives.

To publicize these improvements and assess U.S. Government efforts to secure the global supply chain, our Subcommittee is planning two oversight hearings on March 28th and 30th. In preparation for these hearings, please provide the following information on the Container Security Initiative (CSI) no later than February 15, 2006:

1. Copies of all weekly inspection reports enumerated by each CSI port from February 1, 2005 – February 1, 2006.

2. The yearly expenditures for each CSI port.

3. The number of all Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) employees by port.

4. An inventory and description of all non-intrusive and radiation detection devices utilized by the host country Customs to inspect containers bound for the United States. Please enumerate if these devices have been tested and certified by CBP.

5. All documents relating to "red team" exercises utilized to test the inspections of cargo containers arriving from CSI ports.

6. A list of all instances in which information provided by a CSI team to the host government resulted in a seizure or criminal investigation.

7. Answers to the following questions:

    a. What percentage of maritime containers are screened with a non-intrusive device prior to entering the United States?

    b. What percentage of maritime containers are screened for radiation prior to entering the United States?

    c. What procedures are used to test the non-intrusive and radiation detection devices used in CSI ports? How often is this testing done and how often are the devices certified?

    d. How many radiation hits have occurred at CSI ports? Please list the result of each radiation hit and the procedures followed.

    e. What percentage of containers at CSI ports, which are destined for the U.S., are actually opened and inspected?

    f. If a high-risk container, as defined by the Automated Targeting System, is not inspected at a CSI port, CBP policy dictates that the container is examined upon its arrival at a U.S. port of entry. Please provide the statistics to demonstrate that these high-risk containers are indeed inspected upon their arrival in the U.S.

    g. Of the containers identified as high-risk, what percentage of containers are found to have contraband?

    h. Of the containers randomly identified for inspection, what percentage of containers are found to have contraband?

    i. How many seizures have resulted from the CSI ports? Please provide a list per location.

In addition, please provide the following information on the Customs-Trade Partnership Against Terrorism (C-TPAT) no later than February 15, 2006:

1. The number of C-TPAT applicants.

2. The number of C-TPAT certified companies (Tier 1) and benefits provided to these companies including the ATS score reduction.

3. The number of C-TPAT validated companies (Tier 2) and benefits provided to these companies including the ATS score reduction.

4. The number of C-TPAT validated plus companies (Tier 3) and benefits provided to these companies including the ATS score reduction.

5. A description of the membership process, from the initial application through the certification and validation process. Also, please elaborate on the validation strategy, including the process for re-validations.

6. The number of supply chain security specialists and average grade and pay of a supply chain security specialist.

7. Answers to the following questions:

    a. What derogatory information will prevent a C-TPAT applicant from being certified? Please provide a listing of the types of information that would be considered derogatory to an application.

    b. What percentage of C-TPAT applications are denied? What is the process for a C-TPAT applicant to appeal this decision and re-apply for membership?

    c. How long must a C-TPAT member, which has been removed or suspended from the program, wait prior to re-applying for membership?

    d. CBP revised the minimum security guidelines for importers and is planning to do the same for other aspects of the supply chain. Please provide the timeline for revising the security guidelines for the other sectors of C-TPAT membership.

    e. What percentage of C-TPAT importers' containers are (1) reviewed, (2) examined with a non-intrusive device, and/or (3) physically inspected? Please provide information as to any contraband found during these inspections.

    f. How often are security profiles of current C-TPAT members reviewed?

    g. Has an independent audit been conducted of the CBP validation process? If yes, please provide the results.

    h. Please provide a copy of the automated validation assessment questionnaire. How were the questions used in the assessment generated? Is there a scoring system associated with this questionnaire?

    i. Since the inception of C-TPAT, has CBP observed a reduction in the number of cargo theft incidences?

Thank you in advance for your continued cooperation with our oversight investigation. If you or your staff has any questions regarding this matter, please contact us or have your staff contact Brian White, Professional Staff to the Majority, or Laura Stuber, Counsel to the Minority, with the Senate Permanent Subcommittee on Investigations at (202) 224-3721.

Due to new security procedures, it is necessary to make advance arrangements for the delivery of documents through courier or messenger service. Please contact the aforementioned staff in order to obtain the procedures necessary for delivery.

Sincerely,

Norm Coleman
Chairman
Permanent Subcommittee on Investigations

Carl Levin
Ranking Minority Member
Permanent Subcommittee on Investigations

cc: The Honorable Michael Chertoff, Secretary, U.S. Department of Homeland Security

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

February 3, 2006

VIA U.S. MAIL & FACSIMILE (202/772-9734)

Mr. Vayl Oxford
Director
Domestic Nuclear Detection Office
Department of Homeland Security
245 Murray Lane, S.W.
Washington, D.C. 20528

Dear Director Oxford:

Securing the homeland from Weapons of Mass Destruction (WMD) should be one of our top national priorities. As such, our Subcommittee has closely followed the implementation of programs to confront this threat. In preparation for oversight hearings scheduled March 28th and 30th to examine efforts to detect and interdict a radiological or nuclear weapon, please provide the following information no later than February 15, 2006:

1. The domestic Radiation Portal Monitors (RPMs) deployment strategy at the following border crossing venues:
   a. Land Borders
   b. Sea Ports
   c. Rail
   d. Air Cargo
   e. International Mail and Express Consignment Carriers
   f. International Passengers and Baggage

2. The current (as of 1 February 2006) status of deployment to include the number of RPMs deployed at each of the venues detailed above. Please enumerate what percentage of the total venue is covered with RPMs.

3. Copies of the Memoranda of Understanding (MOU) with DHL, FedEx, UPS, and other private sector entities allowed to screen for radiation. Please provide the audits of these deployed RPMs.

4. DNDO's threat prioritization list of nuclear/radiological materials.

5. The standard operating procedures used by CBP to examine a shipment or vehicle which alarms for radiation.

6. A summary of the test results of the current and prototype next-generation RPMs that were conducted at the Nevada Test Site (NTS) in the fall of 2005.

7. Answers to the following questions:

   a. What is the status of the Domestic Nuclear Detection Office (DNDO) global strategy and architecture for nuclear detection?

   b. What percentage of maritime containers entering the United States are screened for radiation (inclusive of domestic and international screening)? Please delineate this percentage domestically and internationally.

   c. What is the role of the DNDO in the programs and efforts to install and provide radiation detection equipment abroad? How does DNDO coordinate with other federal agencies such as Department of State, Department of Defense, and Department of Energy to fulfill this function?

   d. Describe the relationship between the DNDO and the NRC, specifically as it relates to the materials license process.

   e. What is the official Department of Homeland Security policy on how to utilize the VACIS machine for non-intrusive inspections? Specifically, does DHS recommend that containers are driven through the VACIS or is the VACIS moved over the containers?

   f. Has an evaluation and operational test been conducted of the deployed RPMs? If so, please provide a summary of the results.

   g. Please provide a summary of how many positive alarms for radiation have been recorded by RPMs deployed domestically and indicate which of the alarms are nuisance alarms and which ones have been of threat materials.

   h. What is the number of personnel that have been trained to use the RPMs? Please indicate the number of available and trained personnel at each deployment site.

   i. What procedures are in place to share the results of the radiation screening with other Federal agencies as well as State and Local agencies?

   j. Has any training been offered by DNDO to state or local agencies in the detection of radioactive materials? If so, please specify who conducted the training, the purpose of the training, and the type and length of training as well as the materials provided to the state or local agencies.

k. Has any red teaming been conducted of currently deployed RPMs? If so, please provide the results and testing protocol.

l. What are the current advanced technologies being looked at by DNDO?

Thank you in advance for your continued cooperation with our oversight investigation. We look forward to working with you to strengthen this vital program. If you or your staff has any questions regarding this matter, please contact us or have your staff contact Brian White, Professional Staff, with the Senate Permanent Subcommittee on Investigations, at (202) 224-3721, or Madelyn Creedon, Professional Staff with the Senate Armed Services Committee at (202) 224-3871.

Due to new security procedures, it is necessary to make advance arrangements for the delivery of documents through courier or messenger service. Please contact the aforementioned staff in order to obtain the procedures necessary for delivery.

Sincerely,

Norm Coleman
Chairman
Permanent Subcommittee on Investigations

Carl Levin
Ranking Minority Member
Permanent Subcommittee on Investigations

cc: The Honorable Michael Chertoff, Secretary, U.S. Department of Homeland Security
Ms. Deb Spero, Acting Commissioner, U.S. Customs and Border Protection
The Honorable David Walker, Comptroller General, U.S. Government Accountability Office

APPENDIX B

List of CSI ports as of March 9, 2006 [72]

In the Americas:

- Montreal, Vancouver & Halifax, Canada
- Santos, Brazil
- Buenos Aires, Argentina
- Cortes, Honduras

In Europe:

- Rotterdam, The Netherlands
- Bremerhaven & Hamburg, Germany
- Antwerp and Zeebrugge, Belgium
- Le Havre and Marseille, France
- Gothenburg, Sweden
- La Spezia, Genoa, Naples, Gioia Tauro, and Livorno, Italy
- Felixstowe, Liverpool, Thamesport, Tilbury, and Southampton, United Kingdom (U.K.)
- Piraeus, Greece
- Algeciras, Spain
- Lisbon, Portugal

In Asia and the East:

- Singapore
- Yokohama, Tokyo, Nagoya and Kobe, Japan
- Hong Kong
- Pusan, South Korea
- Port Klang and Tanjung Pelepas, Malaysia
- Laem Chabang, Thailand
- Dubai, United Arab Emirates (UAE)
- Shenzhen and Shanghai
- Kaohsiung
- Colombo, Sri Lanka
- Port Salalah, Oman

In Africa:

- Durban, South Africa

---

[72] *See* CBP website, *http://cbp.gov/xp/cgov/border_security/international_activities/csi/ports_in_csi.xml*, accessed March 15, 2006. The Port of Cortes, Honduras became the 44th CSI port on March 25, 2006. *See* CBP website, *http://www.cbp.gov/xp/cgov/newsroom/press_releases/03252006.xml*, accessed March 27, 2006.

APPENDIX C

Foreign Oversight Trips by
the Senate Permanent Subcommittee on Investigations

DATE	SITE OF INSPECTION
August 18-22, 2003:	Port of Hamburg, and Port of Bremerhaven, Germany
August 7-14, 2004:	Port of Hong Kong, Special Administrative Region of China Port of Singapore, Singapore Port Klang, Malaysia
December 6-11, 2004:	Port of Felixstowe, United Kingdom Port of Le Havre, France Port of Rotterdam, The Netherlands
July 21-28, 2005:	St. Petersburg and Moscow, Russia
August 23-30, 2005:	Port of Tokyo, Japan Port of Hong Kong, Special Administrative Region of China Port of Shenzen, China Port of Shanghai, China
December 9-13, 2005:	Port of Hong Kong, Special Administrative Region of China

APPENDIX D

Domestic Oversight Trips by the Senate Permanent Subcommittee on Investigations

DATE	SITE OF INSPECTION
July 8-9, 2004:	FEDEX Facility, Memphis, Tennessee
February 23-25, 2005:	Port of Los Angeles and Port of Long Beach, California
April 7, 2005:	Port of Norfolk, Virginia Port of Chicago, Illinois
September 28, 2005:	JFK Mail Facility, New York
February 16, 2006:	Port of Newark, New Jersey
February 22 – 23, 2006:	Port of San Ysidro, California