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

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

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

U.S. GOVERNMENT PRINTING OFFICE

27–754 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

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

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

TUESDAY, MARCH 28, 2006

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:32 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Norm Coleman, Chairman of the Subcommittee, presiding.

Present: Senators Coleman, Collins, Domenici, Levin, Akaka, and Lautenberg.

Staff Present: Majority: Raymond V. Shepherd III, Staff Director and Chief Counsel; Brian M. White, Professional Staff Member; Joanna Ip Durie, Detailee, ICE; Mary D. Robertson, Chief Clerk; Leland B. Erickson, Counsel; Mark L. Greenblatt, Counsel; Matthew S. Miner, Counsel; Cindy Barnes, Detailee, GAO; Kathy Kraninger and Allison Boyd (HSGAC/Collins); Henry Abeyta (Energy Comm./Domenici); Minority: Elise J. Bean, Staff Director/Chief Counsel; Laura Stuber, Counsel; Richard Kessler (Akaka); Peter Vallario (Akaka); Madelyn Creedon (Armed Services/Levin); and Wendy Anderson (Lautenberg)

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. This hearing of the Permanent Subcommittee on Investigations is called to order. Good morning and thank you all for being here.

Today we'll be holding 2 days of hearings on perhaps the most important threat confronting our country: Terrorists acquiring and detonating a nuclear weapon in the United States. Have no doubt, this threat is real.

The Director of National Intelligence, John Negroponte, starkly noted this threat in his public testimony last month. "Attacking the U.S. homeland, U.S. interests overseas, and U.S. allies," he said, in that order, "are al-Qaida's top operational priorities. . . . al-Qaida 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. In fact, intelligence reporting indicates that nearly 40 terrorist organizations, insurgencies, or cults have used, possessed, or expressed an interest in chemical, biological, radiological, and nuclear agent or weapons."

While the potential threat of a nuclear bomb is real, we cannot overlook the serious consequences that would result from a dirty bomb. For example, a dirty bomb constructed with Cesium–137, which is significantly less powerful than a nuclear weapon, detonated in New York, would wreak havoc, forcing millions to flee the city, and costing us billions in cleanup costs. It could close down Wall Street.

A disturbing report from GAO that will be part of today's hearing demonstrates significant vulnerabilities in our defenses against a dirty bomb and other terrorist's threats.[1] GAO investigators were able to smuggle enough radioactive source material to manufacture a dirty bomb across our northern and southern borders.

However, there is both good news and bad news to this story. The radiation detectors correctly alarmed, signaling the presence of radioactive material. The Customs officers followed the proper procedures as well. This is the good news.

The bad news, however, is that the officers were fooled by fraudulent documents and didn't have the mechanisms to verify the documents. These are documents that my 20-year-old son could easily develop with a simple internet search using his computer at home. We cannot allow this potentially deadly material to transit our borders with such ease.

Following this report, I am pleased to report that DHS has done the right thing. They have acknowledged the vulnerability and are taking corrective action to ensure that we close this gap. The Nuclear Regulatory Commission (NRC), however, does not appear ready to acknowledge that this is a problem, and I disagree with that. It is a problem when it is tougher to buy cold medicine today, after what we did with the Combat Meth Act—than it is to acquire enough material to construct a dirty bomb.

Many experts, including one here this morning, believe that a maritime container is the ideal platform to transport nuclear radiological material or a nuclear device into the United States. Since 90 percent of global trade moves in maritime containers, we can not allow these containers to be utilized to transport weapons of mass destruction. The consequences of such an event would be devastating to our way of life and our economy.

Therefore, it is imperative that we look at these issues holistically, neutralizing the radiological and nuclear threat and securing the global supply chain. We must, first, secure, detect, and interdict nuclear and radiological materials, and second, ensure the global supply chain is secure.

Our defenses against this threat must start overseas. The first line of defense is securing source material in Russia and the former Soviet Union states. Simultaneous to securing the material at the source, our second line of defense must be to detect and interdict this material if it falls into the hands of a terrorist or if an insider tries to sell this material to a terrorist or a terrorist network.

These initiatives push our borders out, yet concurrent with these efforts, we need to secure material in the United States and detect and interdict material at our ports of entry. The borders of the United States must be the last line of defense. Collectively, this

[1] See Exhibit 5 which appears in the Appendix on page 359.

layered strategy will bring us closer to preventing the nightmare scenario—a terrorist with a nuclear weapon.

For the past 2 years, the Subcommittee has conducted an extensive investigation into global supply chain security and our layered defenses against nuclear terrorism. Today, in the first of our two-part hearing, we will address this layered approach to detect and interdict potential smuggling attempts—both abroad and domestically—as well as our efforts to secure the material domestically. In the second part of the hearing, on Thursday, we will focus on global supply chain security.

I want to take this opportunity to thank Ranking Member Levin, Chairman Collins, Senator Lieberman, and Representative Dingle for their support and interest in this important subject. Preventing nuclear terrorism and securing our Nation's ports demands a bipartisan and bicameral approach.

I will note that Chairman Collins will be conducting a hearing on the broader issue with the full Committee. She authorized the GreenLane Maritime Cargo Security Act. This is really the holistic approach, and I appreciate her leadership on this issue. And I appreciate the opportunity for this Subcommittee to take a piece of it.

The Government Accountability Office has laid the groundwork for today with three superb reports.[1] Collectively, the reports detail many positive steps taken by the U.S. Government to address these issues, but more importantly, note several gaps in our defense. Specifically, 4½ years after September 11, less than 40 percent of our seaports have basic radiation detection equipment. This is a massive blind spot. Pervasive corruption poses a significant challenge to our detection efforts.

And the Nuclear Regulatory Commission, I believe, remains in a pre-September 11 mindset in a post-September 11 world. For example, the NRC has yet to implement even the most basic of reforms to secure radiological material, which I believe the GAO set forth in 2003. And I anticipate asking the GAO about that today.

These issues must be addressed with a sense of urgency. We must close the gap at our ports. The NRC must reform the processes by which anyone can acquire radiological material. And the National Nuclear Security Administration must continue to aggressively build safeguards against corruption.

I would like to welcome Governor Kean, former Chairman of the distinguished 9/11 Commission, and Commander Flynn, to our hearing today. Our hearing will address the efforts to prevent the smuggling of nuclear and radiological materials, the disturbing fact that less than 40 percent of maritime containers entering the United States are screened for radiation, and the ability of undercover GAO investigators to use fraudulent documents to transport enough radiological material across the border to construct a dirty bomb. I look forward to your testimony and an engaging hearing.

I would like to turn to my Ranking Member. I do know Chairman Collins has to be covering the floor on major legislation. But I'll turn to, I think, Senator Levin.

---

[1] See Exhibits 3, 4, and 5 which appear in the Appendix on page 222, 301, and 359, respectively.

Senator LEVIN. Well, Madam Chairman, if you're going to cover the floor, please go ahead. Thank you, though. Thank you, Mr. Chairman.

OPENING STATEMENT OF CHAIRMAN COLLINS

Chairman COLLINS. Thank you, Senator Levin, for your courtesy. As you're aware, the Lobby Reform Act is on the floor today. We're in the midst of trying to work out the final negotiations to allow us to finish that bill today. So I very much appreciate your courtesy.

I want to commend both the Chairman and the Ranking Member for their efforts to strengthen the security of our ports by securing the global supply chain. If terrorists were to obtain nuclear material and smuggle it into this country, the consequences would be catastrophic: A tremendous loss of life and a crippling blow to our economy.

As we learned after the attacks on our country on September 11 when all commercial aircraft was grounded for a time, it is undoubtedly true that an attack on one port would result in all ports being closed for a period of time. That would quickly deliver a crippling blow to our economy.

The Chairman's work builds on the hearings that the full Committee has held on this challenge, beginning 3 years ago. And I commend you for your in-depth investigation into this issue.

Many security experts, including the two experts that are before us on the first panel, have warned that a weapon of mass destruction is most likely to be smuggled into our country via a marine container. The number of containers entering this country continues to grow by more than 10 percent per year. In fact, Customs and Border Protection's latest estimate is that the number arriving by ship exceeds 11 million. Just a couple of years ago when we were discussing this issue, it was 9 million. Now it's more than 11 million.

Given current technology and the sheer volume of traffic, we simply cannot physically search every container without bringing trade to a standstill. The U.S. Government cannot follow every container throughout its global journey, nor can the government track every container and every piece of cargo along the roads, rails, and airways that bring them to the ports.

What we need is a public/private partnership—that was the purpose of the C–TPAT program—and also a partnership with other countries, as we have with the Container Security Initiative (CSI). But previous work done by this Committee and by this Subcommittee have shown that those programs, while well-conceived, have been flawed in their implementation. Indeed, through CSI, only 17.5 percent of high risk cargo targeted for additional inspection actually receives it before being loaded onto ships and sent to our shores.

We are making some progress in deploying radiation portal monitors at our ports. I recently visited the Port of Seattle and saw the trucks rolling through these monitors. I was impressed with the speed. There are quite a few false positives, sometimes caused by kitty litter and marble, but they certainly are a step in the right direction.

But as I watched the trucks with the containers rolling through the nuclear detectors, I couldn't help but think that it's too late by that point. If there is nuclear material or the makings of a dirty bomb in one of these containers in Seattle, we have failed. We need to install radiation detection equipment overseas, at the ports of origin. That is just critical.

But we must be mindful that even if the equipment is functioning properly and in the right place, if it's not administered effectively, the program will not be a success. We see evidence of this concern in the Government Accountability Office reports that the Chairman has commissioned. These reports indicate that corruption and the use of false documents are a problem overseas—findings that are very troubling. It tells me that we need to have more of our own agents and inspectors stationed at foreign ports, and we need to make this a priority.

Again, Mr. Chairman and Senator Levin, thank you for your courtesy in allowing me to proceed. I will be watching the hearing from afar as I continue the negotiations. Thank you.

[The prepared statement of Senator Collins follows:]

PREPARED STATEMENT OF SENATOR COLLINS

Thank you, Mr. Chairman. I commend you for your efforts to strengthen the security of our ports by securing the global supply chain. If terrorists were to obtain nuclear or radiological material and smuggle it into this country, the consequences could be catastrophic: a tremendous loss of life and a crippling blow to our economy. Your important work builds on hearings the full Committee has held on this challenge beginning three years ago.

Many security experts, including notably Governor Kean and Dr. Flynn, who will testify this morning, warn that a weapon of mass destruction is most likely to be smuggled into our country via a marine container. The number of containers entering this country by sea continues to grow by more than 10 percent per year. In fact, Customs and Border Protection reports that in fiscal year 2005, the number arriving by vessel was more than eleven million.

Given current technology and the sheer volume of traffic, we cannot physically search every container without bringing trade to a standstill. The United States government cannot follow every container throughout its global journey, nor can it track every container and every piece of cargo along the roads, rails, and airways that bring them to ports. No one nation can secure the international supply chain.

For that reason, executive branch agencies engage in global initiatives to detect and interdict the illegal transport of nuclear and radiological materials through programs such as the Department of Energy's Second Line of Defense. The deployment of radiation detection equipment overseas, at the borders of nations that are the most likely source of illicit nuclear materials, is a proactive investment in our national security. It is in every nation's best interest to stop smuggling efforts as close to their source as possible.

The United States has set a policy of zero tolerance for the arrival of weapons of mass destruction at our borders. That includes a plan to deploy radiation detection technology at all 380 sea, land, and air ports of entry. The intent is to scan all containers and vehicles entering our country for radiation by 2009. I am interested to hear from our witnesses today about the appropriate mix of detection technologies deployed overseas versus at domestic ports of entry. Clearly, we should detect and interdict these dangerous materials as far from the United States as possible. It may well be too late if a weapon of mass destruction were discovered at one of our major seaports, such as Seattle or Los Angeles.

Just a few weeks ago, I visited both of those ports. The physical size of these facilities and the amount of activity that takes place are startling. So too is the proximity of these ports to major population centers. The Port of Seattle is in the midst of a large urban population, with two stadiums nearby and ferries carrying thousands of passengers each day. The consequences of an attack at a port like Seattle would be catastrophic.

In improving port security, we are always mindful of the need to avoid hampering the flow of legitimate goods. While in Seattle, I watched a line of trucks pass

through the portal monitors exiting a terminal. I was impressed with the speed at which the trucks were able to move. While the current technology is not perfect, CBP has proven that radiation monitors can be deployed without significantly impeding the flow of commerce. I also noted the small footprint required to install the equipment, which seemed to fit naturally into the flow of the traffic. While terminal operators use every inch of possible space to move more containers, they need only travel to Seattle and other places where the equipment is installed to see that security can be increased without sacrificing commercial flow or space.

While progress has been made in deploying a global network to detect and interdict nuclear materials, we will hear today from the Government Accountability Office about continuing challenges. Clearly, in order to be effective, equipment deployed must be properly used. Reports of corrupt personnel at certain foreign border stations and ill-functioning equipment undermine the effectiveness of these programs.

In closing, I wish to voice my support of Secretary Chertoff's decision to make nuclear detection and interdiction a priority through the creation of the Domestic Nuclear Detection Office last year. The GAO's preliminary findings indicate this office has made positive contributions already. Its mission is too important to fail.

Senator COLEMAN. Madam Chairman, again, thank you for your leadership on this issue. And, I know it's going to make a difference. This Subcommittee is pleased to be doing its piece, its small piece. But we really do applaud your overall leadership. So I want to thank you for that.

Ranking Member Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Mr. Chairman, thank you particularly for the great leadership that you're showing in an area which is of critical importance to our Nation, and for your focus of this Subcommittee's attention on the smuggling of nuclear and radiological materials across international borders.

The International Atomic Energy Agency has estimated that as of the end of December 2004, there were approximately 660 known attempts to smuggle nuclear or radiological materials across borders worldwide. Now, those efforts were the ones that have been discovered, and logic dictates that many other attempts have been made and may have succeeded. And just how many is unknown.

The damage which a small amount of nuclear material can do is incredible. Plutonium metal the size of this water glass can destroy a city. It can be easily carried, without danger to the carrier until it is part of a nuclear explosion, so that a very easily carried hunk of plutonium this size can destroy Washington, or any other city, and can be easily transported without danger to the person who is carrying it.

So the vulnerability of our country is clear. The Government Accountability Office will testify today that on two occasions during the last year, using personnel posing as importers, it managed to transport radioactive sources across our Nation's border. And the ease with which the GAO was able to move these materials into the United States should be an alarming wake-up call to all of us, in particular to the Department of Homeland Security, but to all Americans, about the extent of our vulnerability.

The Chairman and Senator Collins have described the dangers and the threats to U.S. security by these materials, and I will not repeat this. And I only regret that I'm going to have to leave in a few minutes for a White House commitment or else I surely would want to be here for the entire hearing, Mr. Chairman.

But again, I just want to ask that my entire statement be made part of the record.

Senator COLEMAN. Without objection.

Senator LEVIN. And thank you for your ongoing and your continuing leadership in this and so many other areas.

[The prepared statement of Senator Levin follows:]

PREPARED STATEMENT OF SENATOR LEVIN

I commend the Chairman for his leadership in focusing this Subcommittee's attention on the smuggling of nuclear and radiological materials across international borders, which is a real and ongoing threat to the national security of the United States. The International Atomic Energy Agency has estimated that as of the end of December 2004, there have been approximately 662 known attempts to smuggle nuclear or radiological materials across borders worldwide. These efforts are the ones that have been discovered. Logic dictates that many other attempts have been made and may have succeeded—just how many is unknown.

The vulnerability of the United States to this threat is clear. The Government Accountability Office will testify today that, on two occasions during the last year, using personnel posing as importers, it managed to transport radioactive sources across our nation's borders. GAO's ease in moving these materials into the United States should be an alarming wake-up call to the Department of Homeland Security and to all Americans about the extent of our vulnerability.

Smuggling nuclear and radiological materials presents two distinct threats to U.S. national security. The first and the most serious threat is that weapons grade nuclear material in quantities sufficient to build an improvised nuclear explosive device are smuggled undetected into U.S. territory. An improvised nuclear device constructed and detonated by individuals with technical knowledge could result in massive casualties and widespread physical and economic damage.

The second threat is smuggled radiological materials which are incorporated into a dirty bomb which, when detonated, could cause widespread contamination. Immediate casualties resulting from a dirty bomb would probably be those killed or injured as a result of the explosion itself. A secondary consequence would be that the radiological material would likely contaminate a large area and result in major economic damage, disruption, and an expensive cleanup.

These serious consequences demand that serious effort be taken to prevent nuclear and radiological materials from falling into the hands of terrorists, criminals, or other non-state actors.

Since the fall of the Soviet Union, the Departments of Energy, Defense and State have worked to secure and consolidate nuclear and radiological materials in Russia and the States of the former Soviet Union. More recently, the United States, Russia and the International Atomic Energy Atomic Agency, have expanded their efforts to address radiological and nuclear materials at risk around the world. Governor Kean notes in his prepared testimony a concern about the slow rate at which these nuclear weapons and materials have been secured. The data suggests that it will take another fourteen years before the material in just the former Soviet Union is fully secured.

In 1998, after recognizing the possibility that materials could be stolen or illegally diverted, even from secure sites, DOE, DOD and the DOS, working with Customs, initiated the Second Line of Defense program to detect and interdict nuclear and radiological materials at border crossings. These are the programs which will be discussed today.

More recently, the Department of Homeland Security has worked to improve U.S. capabilities to detect and interdict nuclear and radiological materials at U.S. land borders and seaports, and initiated new programs, such as the Container Security Initiative (CSI), and the Customs Trade Partnership Against Terrorism (C-TPAT), which will be the subject of Thursday's hearing.

Today, we need to understand the nature of the threat, including who is working to smuggle these materials into the United States and elsewhere, where is the material coming from, where are the vulnerabilities and greatest risks, what is being done, and what more can be done to stop the smuggling. One note of caution is that, as we consider how to stop nuclear smuggling by inspections and other means, we must also consider the needs of legitimate commerce to keep goods moving.

The GAO reports show that much more can and should be done to secure nuclear materials where they are stored, and to prevent these materials from moving across international borders illegally. The nuclear threat is one of the gravest facing this country and the world. The Administration and Congress must provide more re-

sources, more effective attention to the problem, and more international cooperation with our friends and allies to stop the illegal trafficking of nuclear and radiological materials worldwide.

Senator COLEMAN. Thank you, Senator Levin. I want you to know I have a newfound appreciation for the concern about garbage being transported into Michigan after reading the report and listening to your concerns. And I am hopefully that of all the issues we address, it's one that wasn't high on my radar screen until I kind of looked at pictures of material coming in where you couldn't see anything.

And sometimes the most obvious stuff is the stuff we ignore until it's too late. So I just wanted you to know that you have awakened the consciousness of this Chairman on an issue that I know has been of great concern to you.

Senator LEVIN. I really appreciate that. Thank you, Mr. Chairman. We'll get into that on Thursday.

Senator COLEMAN. Senator Domenici.

OPENING STATEMENT OF SENATOR DOMENICI

Senator DOMENICI. Senator and Mr. Chairman, I came today and probably would not be able to spend as much time as I would like. But I thought I would share a few thoughts on this issue of supply chain.

It might not be within the immediate recollection of even our distinguished Chairman that the supply chain of dangerous components as part of a nuclear bomb's potential really fell upon the world when Russia and the United States decided that the Cold War was over. There was a period of time when nobody knew how badly Russia had turned loose the controls they had over material that was dangerous. I mean, it was, Mr. Chairman, literally beyond belief.

The way the Russians secured things was to have a secret city in which all of these items of danger were cast about and used. And the security was not like what we worry about. It was a ring of soldiers. So in other words, a general was in charge of securing it with the troops.

And, the troops at a point in time started disappearing. I think you all remember that. You even alluded to it one time in a speech that there were no more soldiers guarding these places. They just decided to go home.

Well, literally, the supply chain was open. And it was open for a long time. And frankly, the United States didn't know what to do about it, to be honest. We had a strange philosophical dilemma up here. Maybe I would say neo-conservatives would say don't pay the Russians anything to clean up their mess; you're giving them our money. You know that. You know who they were. Others said, it is so risky, we'd better pay them. Even if it's our money going to them and they're not necessarily our friends yet, we'd better do something.

I give you this background because to get where we are, we have gone through the passage of a law called Nunn-Lugar which we just plunked down upon this issue as I just reviewed it for you. And we said, we've got to do something about the issue.

And believe it or not, although it worked, anybody that has read its history will know that it had a devil of a time working. And if you were reviewing it now, Mr. Chairman, you would find that it had so many failures because of bureaucracy that it would frighten you—who stopped it, who started it, who wouldn't do it.

Then we had the issue of who pays for it. Well, you understand much of your testimony is we need more money, as I read what you have to say. Well, we had a problem of the Defense Department wasn't quite sure that as this grew, that it should come right out of the defense budget to pay for cleaning up the stockpile of the Soviet Union and to build security apparatus so you couldn't steal their stuff and circulate it around the world. Why should the military pay?

We have now spent more than $10 billion, if you're interested, on that, and we have invented a whole new system for them that we have put in place through the Material Protection Control and Accountability. It is literally an American-built system that says to the Russian—that's where most of this stuff is, you understand; that's where it came from—it says, let's build ways that we can at least know where the equipment is. Take stock of it.

I had an incident—I was there once and they were showing me that we now do have some cameras to take pictures that show you who came in, who came out. And I looked up, and there was a neat little camera there. And I saw the little purchase—little thing advertising it, and it said, "Made in Albuquerque, New Mexico." Which probably meant the Sandia Laboratory guys were doing a good job building cameras and things.

In any way, that concluded with an astronomical effort on the part of the United States, and I was very pleased to lead it, where we decided to purchase, for $350 million 500 metric tons of highly enriched uranium. Now, that's highly enriched. And you've got to down-blend to use it. It's ready for bomb work.

We bought it. It is what is feeding our nuclear power plants in the United States right now. We bought it. We get it from them under a great agreement. They get paid. But the United States is paying a lot of money into the Russian coffers to get that. But guess what it did? It prevents the building of 20,000 warheads. That's what that did.

Now, that's not your problem of stealing it across borders. That's a big macro global problem. But that's pretty good work. We also bought 38 tons of pure plutonium at the same time in that same deal and said, if we can change its form so it can never be used in a bomb again, we've done something to inhibit the supply chain in a dramatic way.

So my advice, for what it's worth, to those who observed this, and you, Mr. Chairman, as you work on this, is to make sure you try to understand how difficult it is for those who you're calling upon to be participants to find their role within their departments. Because they have to find the money, too. And they have to justify it.

It's still there as to who wants to voluntarily come up with the money and who's saying, why should I come up with it. And I think we're coming full circle again, and I'm not there yet but I'm saying close, as to how much of our money should we be giving them to

do their cleanup and to do their security work when they're doing pretty well now with lots of oil and gas money.

That's going to come into battle, and it probably is being felt there in the State Department and probably impacting on some of the things you think might be happening. Thank you very much.

Senator COLEMAN. Thank you, Senator Domenici.

Senator AKAKA. Oh, I'm sorry. I didn't see Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. As all of us are called upon for so many other things, this is great importance and we've got to be able to devote some time for it. But we are being—I want our expert witnesses to know that the distinguished Chairs do not suggest a lack of interest. But Mr. Chairman, I thank you for calling this hearing and having this focus on what's described as the greatest threat to our national security in the nuclear materials that could be used for weapons of incredible destructive destruction.

As the report issued by the 9/11 Commission—we've just turned on the clock, Mr. Chairman; that's a note of interest, if you don't mind. Thank you—I'm the first among equals here—that Governor Kean, a dear friend and colleague in government for so many years and who has made such a great contribution to our country by his leadership on the 9/11 Commission as well as so many other things that go on in our State and our country, the report card that was issued by the 9/11 Commission last year gave the Bush Administration a grade of "D" for its efforts to secure nuclear materials around the world.

The Commission's report said, "Countering the greatest threat to American security is still not the top national security priority of the President and the Congress." And I recall, Mr. Chairman, when we were talking about budget for DHS and I made reference to Governor Kean's suggestion or recommendation that money for security grants be distributed based on risk, well, we had a vote on this Committee and the issue lost 15 to 1. Guess who the one was.

So the question is: How seriously are we going to take these threats? How much political interest is entered into the equation? I think a lot. But these nuclear terror threats are still out there, and nuclear materials could be smuggled into our countries through one of our greatest vulnerabilities, our ports.

And if you look at the port of New York and New Jersey and see the activity there, you just know that there's a momentum created by the transfer of materials that could obscure or hide lots of things that we wouldn't like to see in our area. Some 9 million cargo containers enter our ports every year, and almost 3 million in the port of New York and New Jersey alone. But we still inspect only 5 percent of these containers. Five percent. Unacceptable, given the threats that we face.

And I share the belief that we need to inspect or scan all containers that enter our country. And no longer is it a thought that it can't be done. It can be done. We've seen it in places like Hong Kong, and we see it in other areas where attempts to create scanning machinery are bearing fruit.

And I strongly support the amendment that my colleague, Senator Menendez, offered to the budget resolution to require 100 per-

cent screening. The alternative is to continue to rely on intelligence, the same intelligence that President Bush relied on in determining whether Iraq had weapons of mass destruction. And we now know that we can't afford to be wrong again.

One nuclear device smuggled into Port Newark in New Jersey could threaten the lives of 12 million Americans. Threats from other weapons of war, like chemical, biological, could similarly create havoc in unimaginable proportion. But we know that this item under discussion can certainly do that.

Since 1991, the United States has invested approximately a billion dollars a year to monitor reactors in the former Soviet bloc from illegal transfer of nuclear materials. Today those reactors are considered relatively secure, but it's believed that almost 50 reactors in other countries still lack adequate security. And most of them are in China, Ghana, Pakistan, and Uzbekistan, according to a list compiled by the International Atomic Energy Agency. There are also research reactors in countries hostile to America, including Iran and North Korea.

Mr. Chairman, our Nation can do better than a grade of D. We know that we can do better than inspecting 5 percent of cargo containers. The Administration needs to heed the warnings of the 9/11 Commission and make this a top national security priority with the funding and the mandate that accompanies that. Thank you very much.

[The prepared statement of Senator Lautenberg follows:]

PREPARED STATEMENT OF SENATOR LAUTENBERG

Mr. Chairman, thank you for calling this hearing and giving us an opportunity to learn more about the greatest threat to our national security—nuclear materials that could be used to build weapons of mass destruction.

The report card issued by the 9/11 Commission last year gave the Bush Administration a grade of "D" for its efforts to secure nuclear materials around the world.

The Commission's report said, "Countering the greatest threat to America's security is still not the top national security priority of the President and the Congress."

Nuclear terror threats are still out there—and they could be smuggled into our country through one of our greatest vulnerabilities: Our ports.

Some nine million cargo containers enter our ports every year—almost three million in the Port of New York and New Jersey alone.

But we still inspect only five percent of these containers. Five percent. That is unacceptable given the threats we face.

I believe we need to inspect or scan all containers that enter our country. The alternative is to continue to rely on intelligence—the same intelligence that President Bush relied on in determining whether Iraq had weapons of mass destruction.

We can't afford to be wrong again. One nuclear device smuggled into Port Newark in New Jersey could threaten the lives of 12 million Americans.

Since 1991, the U.S. has invested approximately one billion dollars a year to protect reactors in the former Soviet bloc from illegal transfer of nuclear materials.

Today, those reactors are considered relatively secure. But it is believed that almost 50 reactors in other countries still lack adequate security.

Most of them are in China, Ghana, Jamaica, Pakistan and Uzbekistan, according to a list compiled by the International Atomic Energy Agency.

There are also "research" reactors in countries hostile toward the United States, including Iran and North Korea.

Mr. Chairman, our nation can do better than a grade of "D." We can do better than inspecting five percent of cargo containers.

The Bush Administration needs to heed the warning of the 9/11 Commission, and make this a top national security priority.

Thank you, Mr. Chairman.

Senator COLEMAN. Thank you, Senator Lautenberg. Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. I want to commend you for holding this hearing, which is very important to me and to all of us. I want to tell you it's a pleasure in welcoming our distinguished and qualified witnesses this morning.

Mr. Chairman, I have a longer statement, and I'll ask that it be entered into the record.

Senator COLEMAN. Without objection.

Senator AKAKA. I'm pleased that we are addressing the critically important issue of nuclear and radiological security. Over the past few years, I've requested several GAO reports that have identified insufficient efforts by the Federal Government to secure and dispose of radioactive sources, both domestic and internationally.

Going back to early 2003, GAO reported to me problems with the Nuclear Regulatory Commission's documentation and licensing, which according to GAO's testimony remain a problem to this day. This is shocking. And I will be discussing with the NRC why this is so and why haven't they implemented the corrective regulations they pledged to do at that time. I also successfully added a provision to the Energy Policy Act of 2005 designed to help secure radiological sealed sources in the United States.

I have some continuing concerns. I'm particularly concerned about the nuclear and radiological security at our Nation's ports because commercial harbors play a critical role in the economy of my home State of Hawaii. My State receives 98 percent of the goods it imports via sea. Hawaii has been successfully using radiation portal monitors at its seaports and airports to screen international cargo and mail.

However, identifying radioactive sources at our borders and ports of entry must be our last line of defense in a layered approach that begins overseas. To be secure, we must identify, interdict, and secure radioactive sources and nuclear materials at their point of origin before they ever reach our shores.

However, as I looked over the findings GAO will present today, I am troubled about the lack of accountability for programs and duplication of effort. The Federal Government has spent more than $178 million to provide 36 countries with radiation detection technologies that are not being used as efficiently nor as effectively as they should. Congress needs specific performance measures, cost estimates, and timelines for international nuclear detection programs.

I'm also concerned about the possibility of duplicative programs in the newly established domestic nuclear detection office and the National Nuclear Security Administration in the area of radiation detection technologies. The new DNDO runs the risk of becoming another layer of bureaucracy on a crowded organizational chart, duplicating technologies being developed elsewhere in the Federal Government, and siphoning off scarce science and technology funds from other programs.

Mr. Chairman, I look forward to hearing the testimony of our witnesses. Thank you very much.

[The prepared statement of Senator Akaka follows:]

PREPARED STATEMENT OF SENATOR AKAKA

Thank you, Mr. Chairman. It is a pleasure to see so many distinguished and qualified witnesses appearing before the Subcommittee today.

I am pleased that we are addressing the critically important issue of nuclear and radiological security. Over the past few years, I have requested several Government Accountability Office (GAO) reports that have identified insufficient efforts by the federal government to secure and dispose of radioactive sources both domestic and internationally.

In early 2003, the GAO reported to me problems with the Nuclear Regulatory Commission's (NRC) documentation and licensing, which according to GAO's testimony, remain a problem to this day. This is shocking, and I will be discussing with the NRC why corrective regulations have not been implemented, as they pledged to do.

I also successfully added a provision to the Energy Policy Act of 2005 designed to help secure radiological sealed sources in the United States.

However, today we are here to discuss the potential of radiological material crossing our borders. And, according to the testimony GAO will present today, as a nation the federal government isn't doing enough to protect our citizens against this threat.

A nuclear or even a "dirty bomb" attack on American soil would cause unimaginable destruction to our society. I am particularly concerned about the nuclear and radiological security at our nation's ports because commercial harbors play a critical role in the economy of my home state of Hawaii. My state receives 98 percent of the goods it imports via sea. Hawaii has successfully been using radiation portal monitors at seaports and airports to screen international cargo and mail. However, I am troubled that the Department of Homeland Security's plan to deploy additional detection technologies has been delayed, and now faces a projected $342 million overrun.

Detection technologies used at US ports are the last layer of defense. The simple fact is that if a nuclear device is already in the US, it's too late. Furthermore, many of these detectors can be defeated by effective shielding techniques. The difficulty associated with detecting nuclear or radiological materials and responding to these threats when they are already present in the United States underscores the importance of preventing these dangerous materials from being smuggled into the United States in the first place.

Identifying radioactive sources at our borders and ports of entry must be our last line of defense in a layered approach that begins overseas. To be secure, we must identify, interdict, and secure radioactive sources and nuclear materials at their point of origin before they ever reach our shores. However, as I read over the findings GAO will present today, I am troubled about our lack of capability in this area.

My first concern is one of accountability. Our nation has spent more than $178 million to deploy radiation technologies overseas at strategic locations. The Departments of Defense, State, and Energy have programs with foreign governments in 36 countries to provide detection technologies at screening locations in order to reduce nuclear smuggling efforts. While there have been some successes, detection technologies are not being used as efficiently nor as effectively as they should, according to GAO. The additional threat of corrupt border officials in some foreign countries further undermines our security. The GAO also found that federal agencies have fallen short in their ability to coordinate with one another. As GAO notes, we need specific performance measures, cost estimates, and timelines for our international nuclear detection programs.

I am also concerned about the possibility of duplicative programs in the newly established Domestic Nuclear Detection Office (DNDO) and the National Nuclear Security Administration in the area of radiation detection technologies. These technologies must be both effective at detecting nuclear or radiological materials and they must operate efficiently enough to expedite and not impede the flow of commerce. The new DNDO runs the risk of becoming another layer of bureaucracy on a crowded organizational chart, duplicating technologies being developed elsewhere in the federal government, and siphoning off scarce science and technology funds from other programs.

Lastly, we need a comprehensive understanding of the threat at the federal, state, and local levels. Intelligence, analysis, and information sharing play a critical role in combating nuclear and radiological smuggling efforts. Our intelligence community must be capable of sharing information rapidly with first responders at the state and local levels.

I look forward to hearing the testimony of our distinguished witnesses. Thank you, Mr. Chairman.

Senator COLEMAN. Thank you, Senator Akaka. And again, thank you for your leadership on this whole issue of nuclear and radiological security. I know how important it is to your State.

I'd now like to welcome our first witnesses to this morning's important hearing: The Hon. Thomas Kean, former Governor of New Jersey, and Chairman of the 9/11 Commission. Governor Kean, it's truly an honor to have you with us this morning. I'd also like to welcome back to the Subcommittee retired Coast Guard Commander Stephen E. Flynn, a Jeane J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations in New York City. Commander Flynn testified before the Subcommittee last May at our hearing on Container Security Initiative, or CSI, and the Customs-Trade Partnership Against Terrorism, or C–TPAT.

I appreciate your attendance at today's hearing and look forward to your testimony and perspective on perhaps the most important threat confronting the United States, and that's nuclear terrorism.

As I stated earlier, today's hearing will kick off 2 days of hearings on Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain. Today we'll assess U.S. efforts to detect and interdict radiological and nuclear material domestically and abroad. Governor Kean has championed the importance of this issue from his perch at the 9/11 Commission and at the Public Discourse Project. Commander Flynn is one of this Nation's preeminent supply chain and homeland security experts.

I look forward to hearing both of your thoughts on this critical issue. As you're well aware, pursuant to this Rule 6, all witnesses before this Subcommittee are required to be sworn. I ask you to stand and raise your right hand.

Do you swear the testimony you are about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Governor KEAN. I do.

Commander FLYNN. I do.

Senator COLEMAN. Thank you. Governor Kean, we'll have you go first, followed by Commander Flynn. And after we've heard your testimony, we'll turn to questions. Governor Kean, please proceed.

TESTIMONY OF THE HON. THOMAS KEAN,[1] FORMER GOVERNOR OF NEW JERSEY AND CHAIRMAN OF THE 9/11 COMMISSION

Governor KEAN. Mr. Chairman, distinguished Members of the Permanent Subcommittee on Investigations, it's an honor to appear before you today with Commander Flynn, who's done so much in this area to make the country safer. And this Subcommittee, under both its past and current leadership, has made a profound contribution to the security of the United States.

Your investigative and oversight work on the question of the safety, secure storage, and interdiction of nuclear materials continues to be a vital part of the Nation's nonproliferation efforts. And I would commend you, sir, for your leadership and the leadership of this Subcommittee.

[1] The prepared statement of Governor Kean appears in the Appendix on page 110.

We made 41 recommendations from the 9/11 Commission. We think every one of those recommendations is important. But we worked very hard, and I think all 10 of us believe this: The most important of all our recommendations is to prevent terrorists from getting access to nuclear weapons because these are the weapons Osama bin Laden promised to get and promised to use.

And we know that he and the leadership of al-Qaida have been working over the years to acquire them, for more than a decade. And we document this in our report. Testifying in a Federal courtroom in early 2001, an al-Qaida member explained his mission: It's easier to kill more people with uranium.

Now, we know al-Qaida's intent. We know they're patient, and we know that bin Laden and al-Qaida plan very carefully. We're not saying, nor do we believe, that a nuclear event is the most likely. Attacks of the kind we probably saw in Madrid or London mark the most likely pattern. But a nuclear event is possible, and it would have profound and incalculable consequences.

It would put millions of lives at risk. It would devastate our economy and change, we believe, our way of life. It must be elevated, therefore, above all problems of national security because it represents, simply put, the greatest threat to the American people. The Commission's report could not be more clear: Preventing the proliferation of these weapons warrants a maximum effort.

Now, how are we doing in this area? What progress are we making? Are we keeping weapons out of the hands of terrorists? The Commission believed, and I know Senator Nunn believes as well, that it is most important, if we can, to secure these materials at their source. The Cooperative Threat Reduction Program, better known as the Nunn-Lugar program, is carrying out very important and useful actions to secure nuclear materials at their source, and in some cases to take these materials and transport them to a secure location. People in government, especially at the Defense, State, and Energy Departments, are working hard to implement these programs, and I commend them for this important work.

So there are on this policy some positive signs. President Bush and President Putin made an agreement in Bratislava last year, and that gave the bureaucracy a push. American inspectors now have additional access to weapons storage sites in Russia. Liability issues, which had delayed efforts to eliminate plutonium from dismantled weapons, seem, as I speak to be getting resolved.

More of the vulnerable nuclear facilities in Russia are receiving security upgrades. The current Defense Authorization Act includes amendments by Senator Lugar that cut bureaucratic red tape and hopefully will speed up the work of Nunn-Lugar. These are good steps, but they are simply not enough.

What is most striking is that the size of the problem still totally dwarfs the policy response of our government. The Nunn-Lugar program to secure nuclear materials in the former Soviet Union is now 14 years old, and about half of the nuclear materials in Russia still have no security upgrades whatsoever. At the current rate of effort, it's going to take another 14 years to complete the job. And is there anybody anywhere who thinks in this country we have 14 years?

This is unacceptable. Bin Laden and the terrorists will not wait. And the challenge is bigger, as you know, than the ex-Soviet Union. Some 40 countries have the essential materials now for nuclear weapons. Well over 100 research reactors around the world have enough highly enriched uranium present to make a nuclear device. Too many of these facilities lack any kind of adequate protection. Now, the terrorists are smart, and they plan, and they'll go where the security is weakest.

Our own agencies need to make protecting the Nation from a possible WMD attack an absolute priority. And we are disappointed to hear, for instance, that the FBI is not further along on preventing weapons of mass destruction. In short, we do not yet have a maximum effort against what everybody agrees is the most serious threat to the American people.

Now, when is an issue a priority? I think everybody knows when it's a priority. It's a priority when our leaders are talking about it. Now, why isn't the President talking more often about securing nuclear materials? Why, apart from the superb efforts of this Subcommittee, why isn't the Congress focused? Why aren't there more hearings? Why isn't there greater member interest? And what about the media? Why aren't the airwaves filled with commentary if everyone agrees that the crossroads of terrorism and nuclear weapons is simply the most serious threat that we are facing in this country?

What we recommend: The President should develop a comprehensive plan to dramatically accelerate the timetable for securing all nuclear weapons-usable material around the world and in securing our ports. He should request the necessary resources that he needs to complete this task. He should publicly make this goal his top national security priority, and ride herd on the bureaucracy so that we can maintain in this country the sense of urgency that we need on this issue.

The Congress should provide the resources needed to secure vulnerable materials and our ports at the fastest possible rate. The Congress hopefully will work with the President to secure as much public support as possible for this effort. In this area, the President and the Congress simply need to work together, and to do so on a bipartisan basis because there is simply, in my view, no higher priority on the national security agenda.

Thank you, Mr. Chairman.

Senator COLEMAN. Thank you, Governor. Commander Flynn.

TESTIMONY OF STEPHEN E. FLYNN, PH.D., COMMANDER (USCG, RETIRED),[1] JEANE J. KIRKPATRICK SENIOR FELLOW FOR NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN RELATIONS, NEW YORK, NEW YORK

Commander FLYNN. Thank you very much, Mr. Chairman. It's an honor to be back here before you today. And I want to thank you, I want to echo what has been said here before, and commend you for your leadership, and that of Chairman Collins, on these critical issues.

[1] The prepared statement of Commander Flynn appears in the Appendix on page 115.

And I'm also very pleased that Senator Akaka and Senator Lautenberg are here. I know they've been such strong voices on the issues of port security and container security that have been an issue that's consumed a lot of my attention, particularly since September 11, but before then when it was unfashionable.

I am especially pleased to be alongside Governor Tom Kean, who of course has provided this Nation such an extraordinary service with the leadership you provided at the 9/11 Commission. I was sort of astonished to the extent at which many Americans didn't want to look closely at that event of that day. I think that's been part of the trauma of it. But I think so many Americans I certainly hear around the Nation are so grateful for the work that you've done, sir. And it's an honor to be with you today.

Particularly, Mr. Chairman, thank you for your outstanding leadership in raising the profile and advancing practical approaches to this complex challenge. You've been hard at work on this issue, I know, long before the Dubai Ports World controversy made this issue of port and container security the hot button issue here in Washington.

I also want to commend the work of Ray Shepherd and Brian White of your staff for their tireless oversight of activities of the U.S. Government on these issues. I would count Mr. Shepherd and Mr. White, along with Kathleen Kraninger and Jason Yanussi, who are on the staff of the Senate Homeland Security and Governmental Affairs Committee, as four of the most knowledgeable individuals on supply chain container security in Washington.

One of the extraordinary things about this issue is it's very difficult to see the forest for the trees. And the tendency is for people to just take pieces of it, whether it's under Committee jurisdictions or whether it's in the bureaucracy. And there's only a handful of folks, like this Subcommittee, who have been trying to rise above it and see its totality.

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

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

The scenario goes this way. Imagine that a container of athletic footwear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut with a mechanical seal that is put into the door's pad-eyes. These designer sneakers are destined for retail stores in malls across America.

The container and seal numbers are recorded at the factory. A local truck driver, though, turns out to be sympathetic to al-Qaida, and he's the guy who's going to pick up the container. On the way to the port, he gets lost, turns into an alleyway, and backs the truck up at a nondescript warehouse, where a small team of operatives pry loose one of the door hinges to open the container so they can gain access to the shipment. This is a common technique in cargo theft.

Some of the sneakers are removed, and in their place the operatives load a dirty bomb wrapped in lead shielding, and then refasten the door. The driver then takes the container, now loaded with the dirty bomb, to the port of Surabaya, where it is loaded on a coastal feeder carrying about 300 containers for the voyage to Jakarta.

In Jakarta, the container is then transferred to an inter-Asia ship, which typically carry 1,200 to 1,500 containers to the port of Singapore or the port of Hong Kong. In this case, the ship goes to Hong Kong, where it is loaded on a super-container ship that carries typically 5,000 to 8,000 containers for a trans-Pacific voyage.

The container then is offloaded in Vancouver, British Columbia. Because it originates from a trusted name brand company that has joined the Customs-Trade Partnership Against Terror, the shipment is never identified for inspection by the Container Security Initiative team of U.S. Customs inspectors located in Vancouver.

Consequently, the container is loaded directly from the ship to a Canadian Pacific rail car, where it is shipped to a rail yard in Chicago, crossing the border somewhere, I think, in your home State, Mr. Coleman. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago area, a triggering device attached to the door sets the bomb off.

There would be four immediate consequences associated with this attack. First, there would be the local deaths and injuries associated with the blast of the conventional explosives. Second, there would be the environmental damage done by the spread of industrial-grade radioactive materials.

Third, there would be no way to determine where the compromise to security took place, so the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Fourth, and perhaps most importantly, all the current container and port security initiatives would be compromised by the incident.

Now, in this scenario, the container originated from one of the 5,800 companies that now belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been certified by their host Nation as compliant with the post-9/11 International Ship and Port Facility Security Code that came into effect on July 1, 2004.

Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors at Hong Kong or Vancouver. Nor would it have been identified by the radiation portal.

As a consequence, governors, mayors, and the American people would have no faith in the entire risk management regime erected by the Bush Administration since September 11. There will be overwhelming political pressure to move from a 5 percent physical inspection rate to a 100 percent inspection rate, effectively shutting down the flow of commerce at and within our borders.

Within 2 weeks, the reverberations would be global. As John Meredith, the group managing director of Hutchison Port Holdings, warned in a January 20, 2004 letter to Robert Bonner, then the Commission of Customs and Border Protection, "I think the economic consequences could well spawn a global recession—or worse."

In short, the stakes are enormous. But there are four factors associated with the scenario that I just laid out that usefully informs the focus of this hearing. First, the threat is not so much tied to seaports and U.S. borders as it is to global supply chains that now largely operate on an honor system because the standards are so nominal.

Second, no transportation provider, port operator, or border inspector really knows what's in the containers that pass through their facilities, and the radiation portal technology currently being deployed at U.S. borders as a part of the Second Line of Defense and Megaports programs can be evaded by placing light shielding around a weapon.

Third, private companies must be part of the solution since they have huge investments at stake. And fourth, the scenario I just laid out involving Vancouver as the offload port in North America highlights that the challenge of securing global supply chains can involve both port security and border security measures simultaneously.

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

The primary conclusion that I reached in researching my book, America the Vulnerable, is that Americans and the West must assume our most critical infrastructures that underpin our economy will become the target of choice for terrorist groups like al-Qaida. This perspective runs a bit contrary to the longstanding view of terrorism that has held that terrorists are mainly interested in symbolic and spectacular acts of violence that kill lots of people.

But this trend towards economic targeting has been growing in Iraq, for instance. Beginning in June 2003, Iraq's energy sector became a primary target for insurgents. By mid-July 2005, nearly 250 attacks on oil and gas pipelines has cost Iraq more than $10 billion in lost revenues. Successful attacks on the electric grid have kept average daily output at 5 to 10 percent below the pre-war level despite the $1.2 billion that United States has spent to improve Iraqi electrical production.

Now, the key here is that we have insurgents who are increasingly learning how to target critical infrastructure, many of them

foreign insurgents who are going to take their skill-set back home. And disruption is a big part of their efforts.

Against this strategic backdrop, I believe there remains too little appreciation within the U.S. Government that global supply chains and the intermodal transportation systems that support them remain a vulnerable critical infrastructure to mass disruption. Instead, U.S. law enforcement agencies and the national security community have been looking at supply chains as one of but a menu of smuggling venues.

Some agencies like my own former agency, the Coast Guard, and the Office of Naval Intelligence have argued that a weapon of mass destruction is more likely to be smuggled into the United States on a fishing vessel, an ocean-going yacht, or a bulk cargo vessel rather than in a container.

Now, this is probably an accurate assumption in the case of a nuclear weapon. A nuclear weapon would be of such high value asset to a terrorist organization that they would be unlikely to surrender custody to unwitting third parties to transport it.

But the opposite reason applies to a dirty bomb, which is more commonly referred to by national security experts as a weapon of mass disruption because its lethality is fairly limited, a factor primarily of the conventional explosives with which it's made.

The radioactive material contained in the bomb would create costly environmental damage and potentially some long-term health risk for those that were exposed, but not immediate deaths. The fact that a dirty bomb is suited for disruption makes it an ideal weapon to set off within the intermodal transportation system precisely because it would generate the kinds of consequences that my scenario portends.

I'm afraid, for the foreseeable future, the material to make a dirty bomb will likely be available throughout the international community despite even stepped-up counter-proliferation. This is because radioactive materials that can be used in the construction of weapons are becoming more widely available as sophisticated medical and engineering equipment are purchased and used throughout the international community.

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

I review in my written testimony the various initiatives that have been undertaken since September 11 by the Coast Guard, CPB, DOE, DOS, and DOD. Overall, these programs have been largely well-conceived by the parent agency or the department that sponsors them. But I do not believe it's appropriate to conclude that all this activity should be confused with real capability.

For one thing, the approach has been a piecemeal one, with each agency pursuing its signature program or programs without much regard for the other initiatives. There are also vast disparities in the resources that the agencies have been allocated.

But most problematic are some of the questionable assumptions about the nature of the terrorist threat that underpin these programs and the poor state of intelligence that underpins the risk management approach that CBP and the Coast Guard are relying upon to decipher high risk and the low risk. Using Secretary

Chertoff's language, they are relying almost entirely on what they know about known risk, with virtually no capability to deal with the unknown risk.

Further, in an effort to secure funding and public support, agency heads and the White House have often over-sold the contributions that these new initiatives are making towards addressing a very complicated and high stake challenge. Against a backdrop of these inflated and unrealistic expectations, the public will be highly skeptical of official assurances in the aftermath of a terrorist attack involving the intermodal transportation system.

Absent change, in the scramble for fresh alternatives to reassure an anxious and angry citizenry, the White House and Congress are likely to succumb to the political pressure to impose draconian inspection protocols that will dramatically raise costs and disrupt the cross-border trade flows.

We can certainly do better than all of this. And I lay out in my testimony a framework that I have testified about before, which I'll just briefly summarize here. It involves several layers.

The first and most important is that at the factories, we move from a C–TPAT, which relies primarily on customs agents to do the job of trying to verify compliance, to one that would use independent third parties overseen by not just customs, our customs agents, but perhaps by an international team of oversight.

Second, continue to explore the ability to track movements of containers and monitor their integrity as they move throughout the supply chain.

Third, and most importantly, I recommended to you an initiative that I know you looked at and saw, Mr. Chairman, in Hong Kong as I think a true model of where we might be able to go, which is that within private facilities overseas, begin the effort of scanning every container for not just radiation, because of their ability to defeat it in the ways that I just laid out, but also for its contents to find big dense objects that don't belong there, and to record what moves through the system so we can both better deter, ideally be able to identify and intercept without false alarms, and ultimately, in the worst case, be able to resolve issues of where something happened so the whole system won't fail.

And finally, we need to do a much better job in coordinating all this activity and giving it the scale of urgency that Governor Kean has laid out so eloquently here today.

In conclusion, at the end of the day, confronting the nuclear smuggling threat requires that we take the post-September 11 security framework the U.S. Government has been developing, largely on the fly over the past 4 years, and quickly move it to the next generation that builds on the original framework. We have a version 1.0. We need a version 2.0.

The three key ingredients in getting from where we are to where we must be is first to recognize that it's a global network that we're trying to secure. Second, that much of the network is owned and operated by private entities, many who have foreign ownership, so the U.S. Government must be willing and able to work with those companies as well as their host governments to advance appropriate safeguards.

And finally, both Congress and the White House should embrace a framework of "trust but verify," in President Ronald Reagan's phrase, based on real global standards and meaningful international oversight.

Thank you, Mr. Chairman, and I look forward to responding to your questions.

Senator COLEMAN. Thank you very much, Commander, and my thanks to the Governor.

But just quickly, your last four points, when you summarize C–TPAT, you said trust but verify. It's a voluntary system today, but you're recommending including a verification piece in there, which we don't presently have. Is that a fair statement?

Commander FLYNN. That's exactly right, sir.

Senator COLEMAN. In terms of monitoring for integrity, in the scenario that you laid out, if in fact there was within that container from the time it's sealed a device, an RFS device, or a monitor that would let us know if that container was opened, that might prevent the disruptive scenario that you laid out. Is that a fair statement?

Commander FLYNN. That is correct. And I think, the dream is that we'd actually have something built into the container. Because the release of radioactive material would happen over time, and that would be ideal, a sensor for that. But certainly something that helps to detect an intrusion would be quite helpful.

Senator COLEMAN. And that technology is readily available today?

Commander FLYNN. It is. The challenge, of course, ultimately managing this technology in a system of millions of containers would require political leadership and a real commitment on the U.S. Government's part. But it's technically feasible and economically viable.

Senator COLEMAN. One of the things that I have found fascinating, Commander, is in working with the private sector in my State in the past. Companies such as Target Corporation and Best Buy, I didn't want to incur any extra cost in the cost of a container.

But today, when I talk to the private sector, they're looking for more uniform standards like this. They understand the risk of the system being shut down. And I think they'd be more inclined to incur costs for security. However, we need leadership in this country to ensure that you have these kind of systems across the board. Does that corresponded with your conversations——

Commander FLYNN. Absolutely. What I hear from a number of chief security officers of some of the biggest companies is they look around and they see because there is no verification process in C–TPAT, they see a lot of free riders. So they're making a case for standards and enforcement and making a real commitment of resources. But as Governor Kean was saying about the terrorists gravitating to the weakest point, they can't secure the supply chain on their dime when others are basically allowed to essentially come in on the fly.

So it's an issue of raising the bar so there is a level playing field for all of them, and therefore we don't put the whole system at risk. Because we don't like to discriminate by companies and say, oh, Target, you're great; everybody else is bad. When the attack happens, we're going to bring it all down.

The other issue is, frankly, C–TPAT, in a curious way, puts all the liability on the private sector. When basically customs inspectors are only focused on a narrow universe of unknown shippers, basically, to examine, if something goes wrong within their supply chain—and no chief security officer can protect against the scenario that I laid out here today as a one-time incident. They just can't do it with existing technology. That whole company's brand goes up in smoke because customs as well as the U.S. Government will be the first to say, you failed to live up to your security obligations.

So I'm hearing increasingly a willingness to go further, to have a set of standards that we can have confidence, to reduce their own liability exposure, and to level the market playing field so we secure the system.

Senator COLEMAN. And you've mentioned the ICIS system in Hong Kong, in which every container is scanned. A concern has been raised—and I want to discuss this more fully, and we will discuss it more fully Thursday.

But one of the concerns being raised is that, well, you can get the scan, but you can't really analyze. You're not really doing an analysis of that. And somehow, that would be a reason for not scanning every container. How would you respond to that?

Commander FLYNN. Well, one of the key things about the Hong Kong project, and I was involved a bit in sort of the thought leader side of putting it together, is that the basic notion is to defeat—the way that I laid out in the scenario was you shield the weapon and we know the existing radiation portal can't find it.

But now you have a very dense object because you surround it in lead. The scan can alarm around a very dense object where it's not supposed to be. Twenty-foot containers and 40-foot containers actually are set to carry the same amount of weight. Typically, you put more heavy things, therefore, in 20-foot so they take up less room on the ship. So you basically don't expect to see very dense material inside 40-foot containers.

The main application as a primary screen is to validate low risk is low risk. And it also solves your kitty litter problem that alarms off because you see the consistency across the load with the manifest.

The problem is the current protocols of how we do this has not been developed yet on the U.S. Government side. When the pilot was undertaken as a private sector initiative, nobody knew whether it could work or not. And yet what it was about was to say, if it's possible to do 100 percent screening, it works better for the terminal if that can be done as a part of its routine instead of disrupting its life. And it should provide a treasure trove of information for customs to work with.

My own—as I see this evolve very quickly, it is as we merge commercial data about what's supposed to be in the container, and the software builds the archival information, it sees in my sneaker scenario—it's seen 40 shipments of sneakers before, and this is the first one that has this object in it. The software will support the analytical job.

So at the end of the day, we're operating a system where we have no data. In Hong Kong last year, the Customs and Border Protection Service inspected about 3,500 containers total in a port that

moved 22 million containers. Now, all those weren't coming to the United States. But in just two of the gates—because it's not just in Hutchison Terminal; it's also in another terminal called Modern Terminal—those two gates have collected to date almost 2 million images.

I think—which is better, a system where we rely on intelligence that's weak to basically look at 3,500 with foreign cooperation, or one that we're gathering much more information and we can enhance our targeting for it? I think most Americans would rightfully choose the latter, particularly when the facilities are willing to put the equipment in and pay for it and maintain it for us.

Senator COLEMAN. And on the back end in your very chilling scenario—I'm going to move from your chilling scenario to the one that the Governor has presented—you talk about shutting down the entire system until we put in place 100 percent monitoring.

I think the reality is we'd be shutting down the system because we wouldn't know where the problem came from; whereas with this system you could at least—you'd have a database and a multiple layer of database. You'd have an image. You'd have an RPM monitor. You'd have a manifest. I presume you have the computer capacity to go back and track it down.

And then you'd have one part of the system you'd shut down, but there would still be integrity in the rest of the system. And I think folks have to understand: We shut down the global supply chain, we shut down the ability to bring cargo containers to this country, we greatly disrupt, absolutely destroy for a period of time, the economy of this country.

Commander FLYNN. Yes. And the world.

Senator COLEMAN. And the world. I'll start with worrying about Minnesota—but that is the reality that we face.

Commander FLYNN. And I think, Mr. Chairman, it's important to realize that there is deterrent value by building this capability. The scenario laid out was the assumption by the terrorists that putting the dirty bomb in the system would disrupt this critical infrastructure, that it would get that response.

As you build the capability to have the system potentially fare better, you basically take that off as an attractive target. And I think the key is to recognize that there is deterrent value in putting safeguards in place. You almost hear that it's hopeless. They're suicide bombers.

They have limited capabilities, and acquiring a weapon of mass destruction could take years. They have a very limited threshold for failure. They're not going to put it in a system where there's a high risk of detection, or even where the consequences are going to be limited, given the alternatives, and we could therefore safeguard this critical network against the worst case scenario by building it.

I think the bottom line is to recognize that it's not about necessarily preventing a conduit for getting bad things to the United States. It's the system itself that is critical and needs to be safeguarded. And that's why it deserves greater priority than it's been receiving.

Senator COLEMAN. And Governor Kean, you've been part of this across the board. You present a very chilling scenario. The first

scenario is of a nuclear weapon. And clearly, the case you're making is we've got to get back to the sources, and still throughout the world there are a significant number of sources that are still not secured. And that presents a grave threat.

In addition, though, if I can go back to your service as head of the 9/11 Commission. If a dirty bomb were to have exploded at the base of the World Trade Center, can you talk about the economic and the emotional impact?

Clearly it would not be a Hiroshima-like effect of taking at one swipe perhaps hundreds of thousands of lives, if not more. But can you talk a little bit about the economic and psychological impact of a nuclear or radiological device being exploded in a high population area?

Governor KEAN. Well, first of all, the psychological impact of just having that go off in a highly populated area. And for instance, in the financial district, that could make parts of that district unlivable for any number of years. Totally disrupt our economy in the process. Terrify residents of urban areas, or any area where a lot of people live together.

I think the psychological, economic consequences of that would be almost impossible to imagine. It's hard to think of something that would be any worse, which is the reason why that kind of scenario is the one that keeps me awake at night.

Senator COLEMAN. We don't have the capacity to lock down all nuclear material. We use a lot of it in construction. We use a lot of it in medical technology. Therefore, the threat of a dirty bomb becomes a great concern. I envision two scenerios: Building a dirty bomb elsewhere and bringing it into this country; or two, bringing in enough material into this country and then construct it here.

In either scenerio, one of the things that we're going to have to do is rely upon foreign companies like the Hutchison company and others. There's been a lot of discussion about that, and I'm not going to get into the Dubai situation, but the reality today is that 80 percent of our ports are foreign operated. The Megaport Initiation is a program in which we work with companies in other countries to do the screening for us.

I'd be interested if you have any kind of reflections as you look at the overall security on this program. Since you've talked about taking a holistic approach to this issue. How should we be looking at this program? How should we be looking at these issues today?

Governor KEAN. Well, I like the old Reagan phrase, trust and verify, because in any system that we come up with, you've got two problems. One is how you acquire the material, and my own view is it's more likely to be acquired in another place and transported to this country. So if possible, you stop the acquisition, or make it very difficult. That may be number one.

But second, of course, we don't know how many nuclear materials have escaped now from various sources or in various parts of the world. And then comes the issue of our borders, of whether or not you can get the kind of system which Commander Flynn was talking about, whether or not again, in my view, you can raise it on the country's radar screen.

I mean, the problem politically I see is that when we studied September 11, there were very good people both in the Clinton and

Bush Administrations who understood the problem, who understood the dangers, who understood what might happen—not necessarily a plane crashing into a building, but what might happen with al-Qaida and terrorism.

But it was here on the priority list rather than up here. I think in this issue that we're talking about, with the exception of yourself, Senator Lautenberg, and others who really recognize this problem, we're in the same status today on this issue. People know it's a problem. Good people are working on it. But they're working on it slowly. They're not saying it's urgent. They're not raising it to the top of their priority level.

And if the worst occurs, I think the reactions, immediate reactions of the people, of the economy, and, frankly, of our—I think we'll rush to judgment on legislation. I think it will be a bad scenario from every point of view.

Senator COLEMAN. Commander Flynn.

Commander FLYNN. If I could just comment, a big part of the formula that I've been involved with in terms of pushing borders out is that you have to work with both the companies as well as the countries which you're in. Most of the efforts to date has been primarily in the traditional format, going country to country. That is, container security is from customs to customs.

I spent a good bit of time at the end of my Coast Guard career in the Caribbean. We have huge problems with corruption, and this is one of the things you're going to have here. That's just a fact of life. In many cases, the industry players have more integrity in the process than you might find in the local countries. They're very much invested in the enterprise they're protecting.

So take the port of Karachi, for instance, which is now going to be half run by Hutchison Port Holdings and the other half by Dubai Port Worlds. You can't get a container out of there to the Middle East unless you run through those two facilities. I'd like to work with those facility operators for that problem.

I worry, as one of the fallout of what we just recently went through Dubai Port World—I mean, this is now the third biggest terminal operator on the planet—that it's going to—well, I think the company will figure out that it's good to be forward-leaning in any event, but let's just say we made the diplomatic element of that more challenging. We need both to work with foreign countries and with foreign companies.

Senator COLEMAN. Senator Lautenberg.

Senator LAUTENBERG. Thanks, very much, Mr. Chairman, for your patience. The question devolves here and I look at the Committee structure and get an example of how things operate. So the question is: What is the urgency of full participation by all of the Committee members?

I want to start off by asking a very simple question of Governor Kean. Thanks so much for all the things that you have done and will continue to do for us. And Commander Flynn, your testimony was invaluable and your research thorough, and we really appreciate that. And I ask you to continue to sound the alarm, as you have.

During the debate on next year's budget, the Senate rejected an amendment that would have required 100 percent screening of

cargo. Governor, is 100 percent screening an essential factor in protecting our country and protecting our people?

Governor KEAN. It is certainly desirable at some level. I'm not a technical expert, as Commander Flynn is, as to know where that falls on the kind of continuum that he was talking about as to what you do internationally and where you screen things. But certainly if we could do it technologically, it would be certainly a step in the right direction.

Senator LAUTENBERG. Well, as we hear Mr. Flynn's testimony, do we shortchange other areas of concern by focusing so much on port security, on containers? I think we have to kind of take a look at the world out there in which we exist and ask the questions whether or not we must go—let me call it modularly and say, OK, this is the most likely case of vulnerability, and start there, put the resources there and put the focus there.

Governor KEAN. Well, I think you're right. And we certainly have to take the technology we have and install it. I mean, when you hear we have technology that can detect a nuclear device, and yet it's not installed in our various ports and at our borders because we can envision—as Commander Flynn said, we did a movie with Sam Nunn to try to alert the country a bit, and the idea we had was that somebody, again coming across in a station wagon from Canada with a small lead shield, and the radiation wand waves over it and doesn't pick up a thing because that technology—we have the technology that could have gotten through that lead shield, but it's just not installed as yet.

So I don't think we have much excuse for being able to do it and having the technology there at our ports and at our borders and not using it.

Senator LAUTENBERG. So we should get on with it. I was down at the port a couple weeks ago, and every time I go there—and I know that you've been there—and you see the activity and the volume of material that is shipped in. And everything, whether it's from sneakers to Ferraris, it's there. And it is a likely place for something terrible to be delivered to our shores.

And particularly when the FBI says that the most dangerous two miles of targets exist between Newark Airport and Port Newark, exist in the country as a target for terrorism. And here these containers are just overwhelming the whole area. You see them wherever you look. To me, there is no excuse for not getting on with this inspection and these structures for process to make sure that we're doing it.

And why hasn't the Administration, in the view of either one of you, worked to develop such a 100 percent screening regime? What could cause this—I'll call it benign neglect?

Governor KEAN. Well, again, I can't—Commander Flynn is the expert on these areas. But it just seems to me that, as I said before, that we get very distracted in this country. Things come at us unexpectedly in the legislative and political arena, and we sort of respond to what hits us. And it's sort of like a boxer described the Olympic Games: When he gets hit in the face, his hands go to his face, and if he gets hit in the stomach, his hands go to his stomach. And they wonder why he never wanted to fight.

We tend to do that, I think, in the political system in the United States. We don't say this is a No. 1 priority, and we're going to stick to it and we're not going to be distracted. There are good people in the Administration working on this, as there are good people in the Congress working on this. But it's not at the top of the priority list.

People aren't saying, as I think the Committee is saying, and I believe and Commander Flynn believes, this is a No. 1 priority. I mean, the common defense of the United States is the reason government was formed. It's the reason we have a government. And if we're not doing this, then we're not doing anything.

And somehow, with the good leadership, I think if you and the Chairman and this Subcommittee and others who understand this and believe it, we've got to somehow demand that the Administration, the leaders of the Congress, the news media, and other people focus on this, if it is the greatest danger, as I believe it is.

Senator LAUTENBERG. Governor Kean, your voice carries a lot of weight, and I urge you to continue to raise it on behalf of the well-being of our country and this world in which we live.

Commander FLYNN. I think there are two pieces to that, that is why we're not—as you well know, our ports have basically been managed as a local/State matter. And so to some extent, it was a federalism argument made initially here that these are in fact assets that belong to the localities, and they should therefore respond—they should be responsible primarily for the security of them.

Although clearly we have a Coast Guard and customs role, the bulk of the resources—that's basically a fly-by visit kind of presence that we've maintained in there because we've had them being State and local matters. And we don't have a national ports kind of a focus. So that's made it very problematic. You ended up with each agency sort of saying, well, what have I got on my shelf to help with this? And there wasn't much.

States and locals weren't in a position to do this because if Baltimore raises its security cost and bar it makes business more attractive down in Norfolk. I mean, this thing screams for Federal standards. And things like dealing with Halifax and Vancouver as potential competitors, that's a Federal role to negotiate this within a hemispheric context because the transportation system will move around to where the costs are least. So that's one real issue.

The other was, which is why I was so thrilled with what has happened in the Hong Kong model, going to the world's busiest port, two of the world's busiest terminals on the planet, and with the support of the CEOs of those two companies, none of whom have ports in the United States but we're vested in trying to explore this, and customs initially believe it would just be impossible to do this without slowing things down. And they got a lot of importers who said, you can't do this.

So the challenge there was to prove it could be done. Now it's how do we adapt our government protocols to deal with the reality that you could have this amount of screening data available? They can't do it without more resources. They need analysts. They need technology, and they—on our end.

So if the private sector ends up, as in this case they're offering to do, to build this infrastructure and to pay for it through a surcharge, maintain it globally, if they produce that capability and our own government isn't capable of processing it, then it's just another embarrassment that the customs has got to face, or Coast Guard or others, because we're going to have the data we can save up and say, you should have seen it. But because we starved them of analysts and starved them of capabilities, we're not going to get there.

Customs and Border Protection has a total of 80 inspectors to manage the C–TPAT program. There are 11,000 companies in application for that, and some of those companies have literally thousands of providers. Now, how can you provide oversight? There are more—I came down on the shuttle this morning. There are more TSA screeners at the Delta shuttle terminal than we are providing for the entire Customs and Border Protection to do this critical job.

And that's where things start to break down, and I really think that at the end of the day, this is going to expose our government to the biggest cost of terrorism, which is the loss of public credibility and confidence when we have the next attack.

Americans gave their government a pass on September 11, I believe. But they expect that everything that can be done is being done to deal with this threat. And they're going to be appalled at what they see, the lack of effort that's still being made on these issues. While good intentions are there, as the Governor has said, we're just not treating with the level of urgency that certainly this Subcommittee is trying to treat it with. Thank you.

Senator LAUTENBERG. Well, to make your point even clearer, in comparison, TSA screeners: We have 130,000 to 150,000 people in uniform trying to protect our security, we're told, the fight against terrorism. We have an additional billion dollars put into the budget for next year for port security.

Isn't that kind of a hard comparison to understand? I mean, if we want to protect people on our shore—we lost 3,000 people on September 11, and it left a mark on this country that we will probably never recover from. To the Chairman's question earlier about what the effects could be if a dirty bomb was placed in the same area, the fact is that people today are still paying a direct health price for that terrible attack. There are people who have respiratory diseases as a result of being exposed there.

And so when we look at a billion dollars for increased funding to examine these containers, does that strike you as being a major step toward solving the problem?

Commander FLYNN. Well, I think the disconnect here is we're an extraordinarily wealthy Nation who's at war. And I think it would strike most Americans, when it comes to what we're doing on the homeland, we're not acting like a Nation at war.

Senator LAUTENBERG. Governor Kean, do you——

Governor KEAN. Yes. I can't say it any better than that. I mean, this is something—everybody's said it from the President on down. This is a longtime struggle. We're fighting a new enemy that is training people in the ungoverned areas of this world as we speak, and plotting in areas where we can't get at them. You can't attack them like we used to attack a nation state. These are, in a sense, entrepreneurs, these people who we're fighting.

And if we don't recognize that and recognize that nevertheless this is a war we're in and we've got to make long-term plans because they've got long-term consequences, then this Nation and our children are going to suffer.

Senator LAUTENBERG. We have to step up to it.

Governor KEAN. Have to step up to it, I believe.

Senator LAUTENBERG. Thank you very much. Thanks for these—our thanks, Mr. Chairman, go to these two people who have devoted so much of their energy and skill to helping protect this country. I for one am grateful, and I'm sure that all of those who are aware of the mission you're on are grateful.

Senator COLEMAN. I want to echo the words of Senator Lautenberg, Governor Kean, and Commander Flynn, because it speaks volumes. We hope that this clear message you're raising will go beyond the confines of this Subcommittee.

We appreciate your questions, Senator Lautenberg, and we appreciate the testimony of the witnesses. Thank you.

I would now like to welcome our second panel to this hearing. Eugene Aloise, Director of the Natural Resources Environment Team, and Gregory D. Kutz, the Managing Director of Forensic Audits and Special Investigations, both at the Government Accountability Office.

Mr. Aloise, I welcome you to the Subcommittee. Mr. Kutz, I welcome you back to the Subcommittee. By my count, you've testified before this Subcommittee, I think, at least six times and assisted us in identifying over $8 billion in waste, fraud, and abuse. So I want to thank that. I note that Mr. Rhodes is also here from the Government Accountability Office.

GAO is here to testify on three reports you have developed pursuant to our request. These reports are an impressive body of work. Two of these reports, on the domestic and international deployment of radiation detection equipment, were led by Mr. Aloise and his team. Mr. Kutz and his team made an invaluable contribution with their undercover operation at our Nation's borders. I am confident that these three reports will lead to reforms at the Department of Homeland Security, the Nuclear Regulatory Commission, and the National Nuclear Security Administration.

I'd also like to thank Stockton Butler, James Shafer, Eugene Wisnoski, Rich Egan, and Andy O'Connell for their contributions to these reports.

Gentlemen, I look forward to your testimony today. As you're aware, pursuant to Rule 6, all witnesses before this Subcommittee are required to be sworn in. I'd ask you to please stand and raise your right hand.

Do you swear the testimony you're about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. ALOISE. I do.

Mr. KUTZ. I do.

Mr. RHODES. I do.

Senator COLEMAN. Mr. Aloise, we'll have you go first, followed by Mr. Kutz. After we've heard testimony, we'll turn to questions.

I would like to know, Mr. Kutz, in my notes here, it says Mr. Ryan. That's a typo, but it demonstrates just how often you and Mr. Ryan are here. But it's great to have you back.

Mr. Aloise, you may proceed.

TESTIMONY OF EUGENE E. ALOISE,[1] DIRECTOR, NUCLEAR AND NONPROLIFERATION ISSUES, NATURAL RESOURCES AND ENVIRONMENT, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. ALOISE. Thank you. Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to discuss our two reports on U.S. efforts to combat nuclear smuggling in foreign countries and in the United States. Together with our March 2005 report on DOE's Megaports Initiative, these reports represent GAO's analysis of the entire U.S. effort to deploy radiation detection equipment worldwide.

The threat of nuclear smuggling is real. According to IAEA, between 1993 and 2004 there were 662 confirmed cases of smuggling of nuclear and radiological materials. Twenty-one of these cases involved material that could be used to produce a nuclear weapon. Over 400 cases involve materials that could be used to make a dirty bomb.

While these cases occurred in other countries, there is concern that terrorists may try to smuggle nuclear materials or a nuclear weapon into the United States. In response to these threats, four U.S. agencies—DOE, DOD, the State Department, and DHS—are installing radiation detection equipment in foreign countries and in the United States.

My remarks will focus on our two reports being released today. Specifically, I will discuss the progress made by and the challenges facing U.S. agencies in installing this equipment in foreign countries and DHS's effort at U.S. ports of entry, and the challenges DHS faces in completing its program.

The first major initiative to deploy radiation detection equipment was on the borders of the former Soviet Union and Eastern Europe. In the mid-1990s, DOD and the State Department provided portal monitors and other equipment to a number of countries, and in 1998 DOE created the Second Line of Defense program.

Today, in addition to the Second Line of Defense program, six other programs—one at DOE, two at DOD, and three at the State Department—have provided equipment and related training to 36 countries. Combined, these programs have spent about $178 million since 1994.

While much progress have been made, these programs face a number of challenges, including possible corruption of border security officials, technical limitations of equipment installed by the State Department and now maintained by DOE, and inadequate maintenance of some handheld equipment.

Regarding possible corruption, officials from several countries we've visited told us that corruption is a big problem within the ranks of border security organizations. Corrupt officials could defeat these systems by turning off the equipment or ignoring the

[1] The prepared statement of Mr. Aloise appears in the Appendix on page 128.

alarms. We face the danger that a $20 bribe could compromise a $200 million system.

To lessen this threat, DOE and DOD plan to deploy communication links between border sites and command centers so that alarm data is simultaneously evaluated by multiple officials. In addition, screening and training of border guards is also planned.

Another problem relates to limitations of the portal monitors previously provided to some countries by the State Department, which makes them less effective in detecting weapons-usable nuclear material because the portals can only detect gamma radiation.

Since 2002, DOE has maintained this equipment, but except for one site has not upgraded it. We have urged DOE to upgrade this equipment because until these sites receive equipment with both gamma and neutron detection capability, they will be vulnerable to nuclear smuggling.

In addition, much of the handheld equipment provided by the State Department and other agencies may not function properly because it is not being maintained. While DOE is maintaining the handheld equipment it has given to other countries, no U.S. agency has maintained about 1,000 handheld detectors that are vital to border officials conducting inspections on vehicles and pedestrians. For example, we observed border guards using handheld equipment that has not been calibrated properly since 1997. This equipment needs to be recalibrated every year.

In addition, no U.S. agency keeps accurate data on the status and location of all the equipment provided by U.S. programs. Without such a list, we cannot assess if equipment is operational and being used as intended.

Turning to the deployment of radiation detection equipment in the United States, DHS has made progress in deploying and using portal monitors and other equipment. But it is significantly behind in its total deployment schedule. As of the end of last year, about $286 million had been spent on this effort.

DHS is deploying radiation detection equipment in the following five phases: International mail and express courier facilities; major northern border crossings; major seaports; southwest border crossings; and all other categories, including international airports, remaining northern border crossings and seaports, and all rail crossings.

These categories were prioritized according to their perceived vulnerability to the threat of nuclear smuggling. For example, major seaports are vulnerable because sea cargo containers are suitable for smuggling. Also, over 95 percent of the cargo entering the United States does so through seaports.

As of December 2005, about 670 portal monitors have been deployed in the United States, about 22 percent of the planned total portal deployment at U.S. border crossings, seaports, and mail facilities. In fact, deployments in mail facilities and the first phase of northern border sites are complete. However, deployments at seaports and southwest border crossings are about 2 years behind schedule. Importantly, deployments at airports and land rail systems have not yet started.

DHS estimates that with the work it has completed, it is screening about 62 percent of container shipments but only 32 percent of

seaborne shipments and about 77 percent of private vehicles. DHS plans to deploy over 3,000 portal monitors by 2009 at a cost of $1.3 billion. This is a massive undertaking.

However, in our view this estimate and time frame are highly uncertain. In fact, our analysis shows that if DHS continues to deploy portals at its current rate, the program is facing a likely cost overrun of about $340 million and will not be completed before 2014.

We found a number of factors that account for this slow deployment. Specifically, delays by DHS in releasing funds to contractors has in some cases disrupted and delayed deployments. In addition, difficult negotiations with seaport operators about where to place portals, especially for rail cars, has delayed work at seaports.

Many seaport operators are concerned that the construction needed to install the equipment, as well as the screening process itself, will slow down the movement of commerce. Mr. Chairman, it is important that DHS resolve this problem at seaports because until it does, our seaports are vulnerable to nuclear smuggling.

In addition, uncertainties exist in the type and cost of radiation detection equipment DHS plans to employ. DHS's $1.3 billion estimate to complete the program is based on widespread deployment of advanced technology portals. However, the prototypes of these portals have not been shown to be more effective than the portals now in use.

Furthermore, when this technology is available, experts estimate it will cost about $330,000 to $460,000 per portal. Currently, portal monitors cost about $50,000 to $60,000 each. Even if future tests indicate that this equipment works better, it is not clear that the dramatically high cost for this new equipment will be worth the investment.

During our review, we found that CBP officers had made progress in using radiation detection equipment correctly and are following inspection procedures. However, we found gaps in the procedures that need to be addressed.

For example, CBP officers lack access to NRC's license database that could be used to verify that shippers of radiological material actually obtained required documentation. As a result, unless nuclear smugglers in possession of faked NRC licenses raise suspicion in other ways, CBP officers could follow agency procedures yet unwittingly allow them to enter the country with illegal nuclear cargo. In our view, this is a significant gap in the procedures that must be closed. My colleague, Mr. Kutz, will discuss in his testimony just how serious a loophole this is.

Mr. Chairman and Members of the Subcommittee, that concludes my statement. I will be happy to respond to any questions you may have.

Senator COLEMAN. Thank you, Mr. Aloise. Very appreciative.

Mr. Kutz.

TESTIMONY OF GREGORY D. KUTZ,[1] MANAGING DIRECTOR, FORENSIC AUDITS AND SPECIAL INVESTIGATIONS, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY KEITH A. RHODES, CHIEF TECHNOLOGIST, CENTER FOR TECHNOLOGY AND ENGINEERING, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. KUTZ. Mr. Chairman, thank you for the opportunity to discuss our undercover operation to test border security. Our operation had three objectives: First, to determine whether the radiation portal monitors worked; second, to observe the reaction of CBP inspectors to our test; and third, to see whether we could beat the system using a ruse. As I discuss our operation, I will address all three objectives, along with several other key facts and findings.

We tested two land ports of entry that had radiation portal monitors installed, one at the U.S.-Canadian border and the other at the U.S.-Mexican border. For each border crossing, we used radioactive sources commonly used in industry and sufficient to manufacture a dirty bomb.

It is important to note, and as Commander Flynn noted, that a dirty bomb would contaminate an area and could result in significant loss of business and cleanup costs. Although the blasts from the explosives could result in some deaths, the dirty bomb generally would not contain enough radiation to kill people or to cause serious illness. Thus, a dirty bomb is generally considered to a weapon of mass disruption rather than a weapon of mass destruction.

We purchased a small amount of our radioactive sources from a commercial supplier over the telephone. To do so, we used a fictitious company and a fabricated story as to why we needed the radioactive sources. Suppliers are not required to exercise any due diligence when selling small quantities of radioactive sources.

Note that we could have purchased all of the radioactive sources that we needed for both of our border crossings with the same fictitious company and fabricated stories. It is also important to note that our fictitious company was located in the Washington, DC area, and that the items that we purchased were shipped directly to our Nation's capital.

In preparing for our operation, we also produced counterfeit documents. First, we searched the internet and found several examples of official NRC documents. We then used commercial off-the-shelf software to counterfeit these documents, which authorized us to acquire, possess, and transfer radioactive sources. We also produced a logo for our fictitious company and a counterfeit bill of lading.[1]

On December 14, 2005, two teams of investigators made a simultaneous crossing of the north and south border. The radioactive sources in the trunks of both vehicles were sufficient to make a dirty bomb. The radiation portal monitors properly signaled the presence of the radioactive sources when we entered the United States from both Canada and Mexico.

---

[1] The prepared statement of Mr. Kutz appears in the Appendix on page 143.

[1] See Exhibit 10 which appears in the Appendix on page 405.

We observed CBP inspectors at the northern border follow their required procedures after the portal alarm sounded. For example, the inspector directed our investigators to a secondary area for a more thorough inspection. The inspector then located the source of the radiation, identified the source, reviewed our documents, and notified his supervisor of the incident. Although most of the required procedures were followed, the secondary inspection conducted at the southern border was less rigorous.

Although both of our vehicles were inspected in accordance with CBP policy, we were able to enter the United States with enough radioactive sources to make two dirty bombs. The CBP inspectors never validated the existence of our fictitious company or the authenticity of the counterfeit bill of lading and NRC documents. We look forward to working with this Subcommittee, CBP, and NRC to improve the security of our Nation's borders. Mr. Chairman, that ends my statement. I look forward to your questions.

Senator COLEMAN. Thank you very much, Mr. Kutz. I understand, Mr. Rhodes, you're here to provide additional information should the questions warrant that.

Mr. RHODES. That's true, Mr. Chairman.

Senator COLEMAN. Let me start with you. Why don't we start with the investigation, and then I want to move to some broader issues with you, Mr. Aloise.

First, I noted in some of the news stories about this that folks in the Department of Homeland Security's Domestic Nuclear Detection Office said that the substance could have been used with limited effects in terms of a dirty bomb. Could you talk about the effects of a dirty bomb? I will follow up with Director Oxford on the next panel, but I'm interested in your perception.

There seems to be a disagreement between the NRC and perhaps the GAO on the impact of dirty bombs and what their effects could be. Had this material been used to create a dirty bomb, and had that dirty bomb been set off at the New York Stock Exchange or set off at the Nation's Capitol, what would be the effect?

Mr. KUTZ. Yes. Let me make a couple comments. Then Mr. Rhodes is our expert; that's why he's here today. But the items that we were able to get, we could have actually gotten much more. We used what we thought was a minimal amount that we could use to make a dirty bomb that would cause disruption and loss of business and chaos, as I think the prior panel discussed.

And so I would defer to Mr. Rhodes on the more technical aspects of that. But again, there were two parts: We took it across the border, and we also had it shipped here to Washington, DC without anyone asking any questions.

Senator COLEMAN. And the issue wasn't really the quality. I mean, the monitors went off with that quality. You could have had a larger quality.

Mr. KUTZ. Correct.

Senator COLEMAN. But in the end, it was the documents that allowed you to get through and past the secondary check. Is that correct?

Mr. KUTZ. Yes. That's correct.

Senator COLEMAN. Mr. Rhodes, could you talk a little about dirty bombs?

Mr. RHODES. The point I'd like to make is last evening when I was driving home, I heard on the radio the term, "It was an insignificant amount." Just to clarify why we used the amount of material we did, ultimately it was 1,250 times the allowable amount, according to the EPA standards. So according to the Environmental Protection Agency, it was not insignificant.

I've also heard statements made about it being comparable to a smoke detector. First of all, the material we brought across is different than what's in a smoke detector, and the kind of radiation that it emits is different. Also, if we were to destroy it, either via dirty bomb or even if we just ground it up and just blew it out the back of a truck with a fan, in Wall Street, for example, it would register. And then the standard operating procedures would go into play.

Concentric circles would start to be sealed up around the city. And if you apply the standard operating procedures for some period of time until it could be cleared up and until it was considered safe to go into the zone of contamination, nobody would be doing any dealing on Wall Street.

They'd have to go to secondary locations or something like that because no one in their right mind is going to say, well, all of our radiation detectors are going off, but we don't think it's very high, or we think it's insignificant, or it seems to us it's only the amount that's in a smoke detector.

Because you have to have the standard operating procedures and you have to make certain that the area is safe and is uncontaminated. At a minimum, you're going to have to wash Wall Street. You're going to have to hose it down to try to clean the material up.

If this is an insignificant amount of material, then I guess those radiation monitors at the borders are set too low because the whole operation was set to trip those monitors, to make certain that they would go off, to make certain that we had to check the secondary procedures. That's why it's a disruption.

Certainly if I took all of this material and I put it in your coffee, Mr. Chairman, you wouldn't like that. If I were to have you hold it in your hand for more than an hour, you would certainly get a radiation burn from it. So this discussion of insignificance in amount is really a function of how do we respond to it. And if we spread it, and the alarms went off and the radiation detectors showed positive, and it was verified, and the isotope came back as being what it was that we used, there would be tremendous impact.

Senator COLEMAN. Let me talk about the amount that you could have purchased. Is there anything that would preclude somebody from buying a thousand smoke detectors? Would that trigger any kind of review regarding concerns about the radiological nuclear material in those? Is there anything that triggers a review by the Federal Government when one purchases even commercial products that have quantities of radioactive material?

Mr. RHODES. The threshold—with respect to what we purchased, we already had some materials from a prior operation that we did. So we purchased a certain amount, below any threshold that anyone would validate the existence of our company or ask any ques-

tions immediately when we got it, to prove a point. We could have actually done that time and time again and accumulated larger amounts, much larger than we actually used when you combine both of our operations together.

Senator COLEMAN. All right. You mentioned that there is no due diligence. Are there any requirement for anyone to check the bona fides of folks who have multiple purchases of material that would have radioactive material?

Mr. ALOISE. NRC allows the applicant who applies for a license and buys a license up to 12 months before they check if that's a valid applicant or not.

Senator COLEMAN. My questions are: What's the minimum threshold for requiring a license? In other words, is it any amount of material? Is there a threshold for certain quantities of material? When does the NRC actually require somebody to get a license?

If you were buying multiple quantities of medical devices that had this material in it, would you have to have a license from the NRC, or even to purchase smoke detectors in massive quantities?

Mr. ALOISE. Well, in terms of other material other than smoke detectors it varies by device, by material. There are varying amounts and varying limits which would require a license, yes.

Senator COLEMAN. In 2003, the GAO recommended that the NRC spent an accounting for generally licensed material. There was also a recommendation for a database for its licenses. Do you know if those things have been implemented?

Mr. ALOISE. The NRC tell us they're working on developing them.

Senator COLEMAN. Still?

Mr. ALOISE. Still.

Senator COLEMAN. There was also a finding that the precise number of sealed sources is unknown. What does sealed sources mean?

Mr. ALOISE. A sealed source is a radiological device that could be used in medical equipment or industry, that could be used in well logging equipment. And it's about that big, size of a cigar, and it's inserted in a piece of equipment.

Senator COLEMAN. And as for the number of sealed sources, do we know those? Is there any information on that?

Mr. ALOISE. There's no tracking of them. There's no precise—I mean, there's hundreds of thousands of them all over the United States in use.

Senator COLEMAN. Was this the subject of a recommendation in the 2003 report to the NRC?

Mr. ALOISE. Yes. We recommended that—regarding licenses, that NRC modify and change its regulations to validate that an applicant applying for nuclear material was a valid applicant before issuing the regulation. This is something some States already do. Some States hand-deliver a license to an applicant to ensure they're a valid applicant.

Senator COLEMAN. The sense I get from my investigators in talking to the NRC, was that there was clearly a concern about nuclear bombs. Now, that should be a focus, especially because of the potential loss of life.

But the sense we got from the NRC was perhaps almost a—I'll use the word cavalier approach to the idea of dirty bombs, that they just didn't kill enough people and they are insignificant—in terms of the scale of things.

In a post-September 11 world, my concern is that the economic and emotional impact of a dirty bomb goes far beyond a simple calculation of loss of life and property. Can anyone respond to that? Mr. Rhodes.

Mr. RHODES. Let me make one point based on the earlier panel's discussion of patience. Yes, there are thresholds even at the NRC where they'll begin to pay attention. They're equivalent to the IAEA thresholds. If we had been patient enough, we could have used this process to get as much material that would have eventually gotten their attention.

The reason—if we are just talking about loss of life, if we are talking about what are called stochastic and non-stochastic health effects, the stochastic are who dies right away—the non-stochastic are the ones who die right away, and the stochastic ones are how many cancers do you have later on.

If they look at that situation and they say, well, we won't have that much leukemia or we won't have that many people dead, it'll just be like a car bomb or something, I think they are indeed missing your point. Your point is that if I do this on the corner of Wall Street at midday, the havoc that it will wreak is unavoidable because emergency procedures will have to go into effect.

No one is going to say, yes, something went off, but it's not that big a deal. They're going to respond as though all events are exactly the same. And I think that's difficult for people who are viewing it purely in long-term health effects to understand.

Senator COLEMAN. And, the same would hold true if you're looking at the Nation's Capitol, or the White House. Just the psychological impact of saying that we've struck a symbol of American authority would have tremendous impact.

Mr. KUTZ. Yes. I would just say this. The Customs and Border Protection's reaction to our test was very positive, and I think they're proactively looking at solutions to the counterfeiting issue. I think ultimately NRC came around to the fact that the counterfeiting issue was something they need to deal with. But the level of concern and threshold, I just don't think that they were thinking——

Senator COLEMAN. And I was going to follow up on the documents, Mr. Kutz, and I think I mentioned in my opening statement that the technology that you used to create those documents was not some super-secret, high tech, government-only technology. Is it fair to say that a somewhat adept 20-year-old who's pretty good with computers could have created the same documents you created?

Mr. KUTZ. Yes. We used off-the-shelf software, and we used the internet. So it's basically technology anyone could achieve. And actually, I was able to go out—you talk about low technology, I was even able to go on the internet and find the document that we counterfeited. And there are no special security features in these documents that make it difficult to counterfeit them.

Senator COLEMAN. And basically, you could go onto the NRC site, you could see what the documents look like, and then simply recreate those?

Mr. KUTZ. No. They weren't on the NRC site. You had to actually search for other sites. They were on other different sites. NRC does not put them on their site, which we certainly agree with them on that.

Senator COLEMAN. The good news is that Homeland Security is saying that within 45 days they will close this loophole. Are they working with you on that?

Mr. KUTZ. Yes. They've reacted positively. I mean, they're either going to have to have an online capability to validate whether a license is genuine or authentic, or some sort of a telephone system to call in and validate whether the license is legitimate.

Senator COLEMAN. Mr. Aloise, I want to go back to our second line of defense programs, but it's really our first line of defense, which is outside our borders.

Mr. ALOISE. Right.

Senator COLEMAN. That's really where this begins. It begins if you listen to Governor Kean locking down nuclear material abroad. There is still a lot out there, and where there is a lot of this material, making sure that it's not smuggled from there to somewhere else.

And one of the concerns is corruption. And that's noted in your report. Is that correct?

Mr. ALOISE. Yes.

Senator COLEMAN. So how do you deal with that? What can the State Department do? How do you deal with the reality that you can bribe somebody and somebody could turn a blind eye and allow this material through a transit point.

Mr. ALOISE. Well, first of all, everywhere we went on our travels, both U.S. officials and country officials raised corruption as a big problem. And what DOE and DOD are doing are trying to devise systems where the alarm would ring—when it rings at the portal, it will also ring at various levels within the agencies and within the countries themselves that are monitoring the portals.

It will be multiple levels of officials, multiple levels of authorities. So there will be multiple checks, and there won't be just one check with the border official at the portal monitor.

Senator COLEMAN. Just so I understand the technology, if you could have one border, say, on the Russian side, and another border in another country on the other side, if all of a sudden the monitor goes off on one side, a central place can actually see that a monitor has been shut down?

Mr. ALOISE. Yes. They'll be able——

Senator COLEMAN. And could react to that?

Mr. ALOISE. They're building those kinds of systems. Also, they're doing redundant systems. Where they suspect corruption is really bad, they'll put systems on one country and on the other country so they'll get them at both places.

Senator COLEMAN. One of the debates that we're generally having is working with foreign companies. For example, our Megaports program works with foreign companies and in Freeport, works with

Hutchison Port Holdings. Rather than work with the government, you're working with foreign companies operating the terminal.

Have you looked at that? The sense I got from Commander Flynn was that there may be more reliability and an ease of operation in working with these foreign companies than there is working with foreign countries. Can you respond to that?

Mr. ALOISE. Let me say this first. With all of these nonproliferation programs, there is a risk. And the Congress has decided to accept that risk because to do nothing is not acceptable.

And in most of these programs, we're relying on the people in these other countries to operate and maintain and sustain this equipment. And so we've supported these programs in the past, we're on record supporting them, and we still support them. And I think what you have to do is get the buy-in, as Commander Flynn said, of these other countries and companies because they all have a vested interest in this.

Senator COLEMAN. You've raised some concern about the ability of Homeland Security to put in place the radiation portal monitors by 2009. I think there's been a differing of figures. I have some figures that talked about 740 to date, and a plan for about 2,400 by 2009.

Your concern is you would call their ability to do that highly uncertain. Is that correct?

Mr. ALOISE. Right. Right now their deployment rate for portal monitors is about 22 per month, and they would have to go up to about 52 per month to meet their date based on our analysis. And we used their very latest figures from their December 2005 progress report.

Senator COLEMAN. Is there anything that you can see in terms of funding commitment, manpower commitment, or anything else that would give you confidence that they could in fact double the rate at which they're installing these radiation portal monitors?

Mr. ALOISE. Well, our analysis shows that right now one of the biggest problems is the delay in getting the funds to the contractor. There are 13 seaports where they actually had to delay site work to install the equipment because they had not gotten their funding yet. They had to lay people off in some instances. So the first thing we'd like them to see is get the funding out that they already have quicker to the contractor.

Senator COLEMAN. Is there anything that needs to be done legislatively, or is this simply the bureaucracy picking up the pace at which it operates?

Mr. ALOISE. I think it could be done within the bureaucracy.

Senator COLEMAN. One of the other concerns raised in the report was the difficulty in negotiating with port operators. A reality here is that folks are hesitant to change a system and impact the flow of commerce, because time equals money in these operations. Again, it was Commander Flynn who talked about if it's quicker to operate in another port or another country, you're going to do that. You could go somewhere in the United States. You could go to Canada; you could go to Mexico.

But with this issue of negotiating with port operators, did you look at whether in fact there was a legitimate concern that construction, screening, putting and installing radiation portel mon-

itors, would actually slow down the process and cause some negative economic impact?

Mr. ALOISE. In every place we went across various countries around the world and all the ports that we went to in the United States where this equipment is installed, we talked to truck drivers. We talked to seaport operators. No one said to us that this equipment, our screening process, has slowed down commerce. No one has ever raised that to us. It is a big concern, but where this equipment exists, we haven't seen it happening.

Senator COLEMAN. The concern is oftentimes on the part of the private side, the port operators themselves. And as I understand the strategy of DHS—and what they're trying to accomplish—they're trying to work in a cooperative way. They're not putting heavy pressure because they could, in effect, put some very heavy pressure and say, hey, unless you do this now, you're going to suffer these negative consequences.

Is that fair? Do they have the authority to do that?

Mr. ALOISE. Right.

Senator COLEMAN. But they've chosen not to. Do you think we've reached a point where in fact they have to be a little tougher and a little more aggressive, understanding that the concerns about economic impact seem to be somewhat questionable? Have we reached the point where we need the agency to be tougher and more aggressive and simply say to these port operators that this is something we need to do because this is a national security issue?

Mr. ALOISE. Mr. Chairman, I think we're at the point where we're thinking, we need to think outside the box here. We understand why they're negotiating. That makes sense. But they're 2 years behind in their seaport deployments, and they have to take a different approach.

Senator COLEMAN. And 95 percent of the cargo coming into this country comes in through the seaports. Is that correct?

Mr. ALOISE. Right. That's correct.

Senator COLEMAN. So the good news is certainly at our northern and southern borders, we've got good screening, good RPMs in place?

Mr. ALOISE. Yes. At the first phase at the northern border.

Senator COLEMAN. And in fact, Mr. Kutz, when your team went in through the northern border, the alarm was sounded and, in fact, folks were stopped.

Mr. KUTZ. Yes. And they followed the procedures that they were supposed to.

Senator COLEMAN. And yet the material still got through.

Mr. KUTZ. Yes.

Senator COLEMAN. And then at the southern border are those the boxes containing material?

Mr. KUTZ. Yes.

Senator COLEMAN. The southern border also, I think it's fair to say that we've made progress at the southern border?

Mr. KUTZ. Made progress.

Senator COLEMAN. But again, 95 percent of the cargo comes through seaports, and that's where we're significantly behind?

Mr. ALOISE. That's correct.

Senator COLEMAN. I hope the message is that we have to pick up the pace when it comes to seaports.

Gentlemen, thank you. It's been very helpful. I appreciate it.

The final witnesses to our hearing today are David G. Huizenga, the Deputy Assistant Secretary at the National Nuclear Security Administration; Vayl Oxford, the Director of the Domestic Nuclear Detection Office of the Department of Homeland Security; and Jayson P. Ahern, Assistant Commissioner at U.S. Customs and Border Protection.

As I previously mentioned, the purpose of this hearing is to assess U.S. efforts to secure, detect, and interdict radiological and nuclear material domestically and abroad. The GAO has laid the groundwork for this panel, and identified several issues of concern.

Mr. Huizenga, I'd like to thank you for your stewardship of our programs to detect and interdict radiological and nuclear material abroad. In particular, and I'm going to talk about this in my questioning, the Megaports Initiative is a forward-looking program that enhances our collective security by pushing our borders out.

Mr. Oxford, even given your short tenure at DNDO, we're impressed with your leadership and expertise you have brought to the issue of nuclear detection, and appreciate the fact that there is an office, a domestic nuclear detection office. I think that's one of the advancements, one of the improvements that we made that we really haven't talked about but I think puts us in a position to be much better at what we need to do here.

And Mr. Ahern, while unacceptable gaps remain at our seaports, we do acknowledge your yeoman's work at CBP, and specifically your leadership in transitioning CBP from its focus on interdicting guns and drugs to interdicting weapons of mass destruction. I appreciate your attendance at today's important hearing, and I'm anxious to get your response to the issues raised by GAO.

Before we begin, pursuant to Rule 6, all witnesses before this Subcommittee must be sworn in. Please raise your right hand.

Do you swear the testimony you are about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. HUIZENGA. I do.

Mr. OXFORD. I do.

Mr. AHERN. I do.

Senator COLEMAN. Mr. Huizenga, we'll have you go first, followed by Mr. Oxford, and finish up with Mr. Ahern. After we've heard testimony, we'll turn to questions. There's a timing system; when the yellow light goes on, finish your statement. We'll enter your full statements into the record in their entirety.

Mr. Huizenga, you may proceed.

TESTIMONY OF DAVID G. HUIZENGA,[1] DEPUTY ASSISTANT SECRETARY, NATIONAL NUCLEAR SECURITY ADMINISTRATION

Mr. HUIZENGA. Thank you, Mr. Chairman. And thank you specifically for your continued support of these important national security matters. I'm pleased to appear before you today to share the

[1] The prepared statement of Mr. Huizenga appears in the Appendix on page 152.

progress that we made under the National Nuclear Security Administration's Second Line of Defense program, which deploys radiation detection equipment at strategic international locations.

I'd like to note first Senator Domenici's and Governor Kean's pointed remarks about the fact that we have a first line of defense as well, to secure the nuclear material where it is. For more than a decade, NNSA has secured nuclear materials and weapons at over 100 research, storage, and manufacturing facilities in Russia and other countries of the former Soviet Union.

These security upgrades are the first line of defense in our government's strategy to deny terrorists access to a nuclear weapon or the essential material to make a weapon, the fissile material. Backed by strong congressional support and commitments made at the 2005 Bratislava summit, we are on track to complete these security upgrades by the end of 2008.

But the focus of today's hearing is on the Second Line of Defense program, which forms a key element in the multi-layered strategy and system to protect the homeland from an attack using a nuclear or radiological dispersal device. Our international efforts are centered on the premise that confronting the threat of nuclear terrorism as close to the source of the material as possible is the most effective means to reduce the risk of attack.

The Second Line of Defense program pursues its goal to detect nuclear trafficking by partnering with foreign customs and border patrol officials. We provide the host country with a comprehensive system, including detection equipment, training, and support for maintenance and repair of this equipment. We coordinate our efforts closely with other U.S. Government agencies, such as the Departments of State and Defense, our partners at Homeland Security, as well as international partners like the International Atomic Energy Agency.

The Second Line of Defense program has two main components, and I'll address both. First, the Core program. Under the Core program, we have worked cooperatively with Russia and their Federal customs service since 1998 to secure their approximately 350 points of entry and exit against nuclear smuggling. We have provided radiation detection systems at two-thirds of the 120 border crossings, airports, and seaports that we've agreed with them to equip. Our Russian partners have already completed 120 sites on their own, and will fund installations at the remaining border crossings.

While work in Russia remains one of our top priorities, we realize the deployment of radiation detection systems is also needed along other potential smuggling pathways in other countries. Working with the State Department and other agencies to prioritize our efforts, we have expanded the SLD program and are now installing or have installed equipment throughout the FSU and Eastern Europe. We have identified approximately 230 sites in 29 countries outside of Russia, and over the next 3 years plan to complete installation of detection equipment in all high priority countries.

In parallel with providing systematic country-wide detection capability, we're also providing maintenance and repair for the radiation portal monitors provided by the other U.S. Government agen-

cies to 23 former Soviet republics and central European countries from the period of 1992 through 2002.

As Mr. Aloise pointed out in the recent report, the GAO is recommending that these older detectors which can only detect gamma radiation be upgraded with up-to-date gamma neutron detection capability. We have accepted this recommendation and will replace the equipment by the end of 2007.

I'd like to address one other issue that has come up relative to the GAO report, and that is the issue of corruption in these foreign countries. The SLD program is specifically structured to address this concern and this challenge by ensuring, as Mr. Aloise pointed out, that radiation portal monitors will be networked, and more than one official will be involved in closing out an alarm. We will construct central alarm stations, and indeed are working to also connect some of these central alarm situations to regional or national centers.

I'd like to turn now to the other area of Second Line of Defense, the Megaports Initiative. In 2003, we established this program to provide early detection of illicit trafficking of nuclear materials before they enter our territory. We install comprehensive radiation detection and communication systems at foreign ports to enhance interdiction capabilities of the foreign customs authorities.

The program is designed to scan imports/exports and as much transshipment cargo, containerized cargo, as possible while posing minimal impact on terminal operations. Agreements with host governments require all information associated with illicit trafficking of nuclear or radiological materials be provided to the U.S. Government.

We've made steady progress over the last 3 years, identifying approximately 70 ports of interest in 35 countries. We're operational in the Netherlands, Greece, and Sri Lanka, and are conducting a pilot activity in the Bahamas. We will be fully operational in Spain in the spring of 2006 and are at various stages of design and construction in nine additional countries. And we are aggressively pursuing agreements with many of the other remaining 21 countries of interest.

An integral element of the U.S. maritime security strategy, the Megaports Initiative complements the efforts of CBP's Container Security Initiative. Under an April 2005 memorandum of understanding with CBP, we're working closely with our CSI partners and have committed to install radiation detection equipment at all CSI ports.

The radiation detection equipment provided under Megaports reinforces CBP's targeting, screening, and non-intrusive scanning activities. It's not a replacement of it. This is an additional added layer of support.

Earlier, we heard from Commander Flynn that there is a need for greater coordination. And I would just like to point out that we have, I think, coordination at the highest levels of our agencies. I know recently Secretary Bodman had a phone call with Secretary Chertoff in advance of the Secretary's trip abroad, his Asian trip. And as a matter of fact, Secretary Chertoff in his press conference today was talking about the partnership between Megaports and his efforts at Homeland Security.

For the record, I believe it's important to make clear that we have been working very closely with our partners at Homeland Security for some time over the last few years, and will continue to do so.

I'd like to turn briefly to the type of equipment being deployed for primary inspections under the SLD program. The portal monitors were initially developed to ensure nuclear material security at DOE weapons sites. The detectors employ plastic scintillators and helium-3 gas, and have been evaluated at DNDO's test facility in Nevada, and have proven to be operationally effective in harsh and often remote international environments.

That being said, we recognize that the use of this technology places additional burdens on secondary inspectors, and there's a need to develop equipment that will identify radioactive isotopes associated with innocent alarms. We are particularly interested in the Advanced Spectroscopic Portals being developed and tested by DNDO, and I hope that these monitors will be used in secondary inspections at Megaports as soon as they're available.

We have also been working closely over the last 2 years with CBP to evaluate the effectiveness of the Integrated Container Inspection System, or ICIS, mentioned earlier in the hearing. It's being piloted by private industry in the port of Hong Kong. This system combines radiation detection with container identification and non-intrusive imaging, and we support the private sector's efforts to enhance the security of maritime trade lanes. We believe that the private sector container scanning effort is compatible with the Megaports mission.

To contribute to this partnership, we are prepared to provide radiation portal monitors, which we have already purchased and are ready to ship, and a communications package to transmit alarm data to the host government as well as to the CSI officials.

As the primary agency responsible for international deployment of radiation detection equipment, we are working very closely with our DNDO partners to shape the global nuclear detection architecture. Our work with DNDO falls into the following major areas: We're baselining and identifying gaps in the global architecture; identifying operational needs that drive research and development efforts; we're identifying the possible DNDO procurement vehicles, which we may piggyback on their efforts so that we don't have to duplicate procurement efforts at DOE; and we're also looking at sharing overseas data and information with DNDO.

In closing, I would like to restate that the SLD program, or Second Line of Defense program, is dedicated to preventing international smuggling of nuclear and radiological material. We accomplish this goal by working closely with foreign governments and maintaining strong relationships with other U.S. Government agencies. We firmly believe that the unique capabilities of each department and agency are being leveraged to accomplish our common objective of preventing nuclear material from reaching the shores of the United States.

Thank you for your continued support, Mr. Chairman. At this point, I'd be happy to answer any questions.

Senator COLEMAN. Thank you, Mr. Huizenga. Mr. Oxford.

TESTIMONY OF VAYL OXFORD,[1] DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE, DEPARTMENT OF HOMELAND SECURITY

Mr. OXFORD. Good morning, Mr. Chairman. It is my pleasure to come before you today to address how DNDO is responding to the threat of nuclear and radiological terrorism. I would like to thank this Subcommittee for its attention to this issue. I'd also like to take the opportunity to thank the 180,000 people of DHS who are responding daily to the challenges of the post-September 11 world.

Today I will discuss topics related to the use of technology to detect nuclear and radiological materials that could be used in a terrorist attack. I'll review DNDO's accomplishments and some of our program priorities. I will touch upon the progress we have made with Customs and Border Protection regarding the domestic deployment of radiation portal monitors, and how DNDO and DHS as a whole is considering innovative ideas like the Integrated Container Inspection System, or ICIS, that is being piloted in Hong Kong.

First let me address some of DNDO's accomplishments since its founding. As you know, DNDO was established as a joint office in April 2005 to integrate the Department's efforts against the nuclear and radiological threat under a singular authority, and to coordinate those efforts with relevant partners across the government.

DNDO was assigned the responsibilities to develop a global nuclear detection and reporting architecture; to develop, acquire, and support the deployment of the domestic nuclear component of that architecture; and to fully characterize systems' performance before they are deployed. We were also asked to establish protocols and ensure that detection leads to effective response. Finally, we were asked to conduct an aggressive transformational research program to address additional architectural gaps.

In the last year, the DNDO has taken major steps towards achieving its mission. We completed the first ever global detection architecture that allowed us to identify international and domestic vulnerabilities and priorities. We have completed additional development efforts on the next generation passive detection system that would not only detect presence of radiation but will also discriminate between threat and non-threat materials.

We have now completed two high fidelity test and evaluation campaigns at our Nevada test site to characterize systems performance in next generation passive portals as well as handheld mobile and backpack detection systems. Finally, we have begun the development of the next generation radiography system to deliver imaging systems that will automatically detect high density material in cargo.

The DNDO is also taking steps to improve nuclear detection capabilities within our Nation's borders. We have launched the Southeast Transportation Corridor pilot program to deploy radiation detectors to weigh stations and other sites, and to provide training, technical reachback, and operational protocols needed at the State and local level to ensure that detection technology is

[1] The prepared statement of Mr. Oxford appears in the Appendix on page 163.

being operated properly and that alarms are escalated as appropriate.

We are also launching a Securing the Cities Initiative aimed at enhancing protection and response capabilities in and around the Nation's highest risk urban areas. We will work with State and local officials to develop urban and regional deployment and operations strategies, identify appropriate detection equipment, establish the necessary support infrastructure, and develop incident management protocols to respond to a dirty bomb attack. These two initiatives, when integrated, form the basis for the DNDO vision for an interior layered domestic detection framework.

Regarding RPM deployment strategy, this Subcommittee has expressed particular interest in the progress of RPM deployment at U.S. POEs. Additionally, the GAO reports we heard about earlier contained recommendations pertinent to DNDO that I would like to take the opportunity to address.

In its report, the GAO made two specific recommendations regarding the DNDO. It called for the Secretary of Homeland Security, working with the Director of DNDO, in concert with CBP and PNNL, to devise a plan to close the gap between the current deployment rate and the rate to complete deployments by September 2009.

Second, it cited that once the costing capabilities of advanced technology portal monitors are well understood, and before any new equipment is purchased, the Secretary of Homeland Security will work with the Director of DNDO to analyze the benefits and costs of deploying advanced portal monitors.

The DNDO concurs with both of these, and let me address them individually. In the first recommendation, we are working with CBP to propose a deployment strategy that now results in screening of 98 percent of all containerized cargo crossing the southern border by the end of this fiscal year; 93 percent of all cargo crossing the northern border will be complete by 2007; and 98 percent of containerized cargo coming into U.S. seaports will be complete and scanned by the end of 2007. This strategy will result in full coverage of all incoming containerized cargo at every port of entry in the United States by 2011.

We also fully concur with the second recommendation, that calls for a deliberate process to ensure that funds are used in a responsible manner, and that advanced systems with higher procurement costs are deployed in cost-effective situations. The DNDO testing of these systems at the Nevada test site has since validated that systems performance when compared with current systems, and demonstrated in some cases a four times improvement in performance against threat objects, and a 60-percent reduction in false alarms created by naturally occurring radioactive materials.

This information is now guiding a joint DNDO–CBP analysis in support of a revised RPM deployment strategy that is an optimized mix of current and next generation technologies balancing our need for better capability and coverage across the country as well as their associated costs. Initial results of this analysis support the decision to acquire over 600 detection units in fiscal years 2006 and 2007, including 184 current generation RPMs and 106 next genera-

tion portal systems this year, and 131 current generation and 142 next generation systems in the year—fiscal year 2007.

Regarding the integrated cargo inspection system this Subcommittee has witnessed in Hong Kong, first of all I would like to applaud the private sector for creating such a concept for screening international containers. The screening can be compatible with the U.S. Government's layered security strategy, and is another tool to further our ability to identify and address risks. An integrated cargo inspection system, one that combines targeting, passive, and active detection and information analysis, would be a robust contribution to the nuclear detection challenge we face.

The ICIS pilot serves as a model comprehensive passive and active inspection, as well as a model for public/private partnership. However, ICIS, as deployed, is not an operational system. DHS has sent teams to observe the ICIS pilot, and has determined that the technology has potential but still faces significant limitations.

DNDO certainly favors an integrated systems approach where at international seaports every cargo container could be both passively and actively scanned. This would enable us to detect unshielded or lightly-shielded materials with the current and next generation RPMs, as well as automatically detect highly-shielded threat materials using radiography.

Detector data would then be analyzed by DHS prior to cargo transit, and along with ATS, manifest, and detector data, would be integrated for enhanced targeting capability. Additional targeted inspection could be performed upon arrival at U.S. POEs utilizing mobile advanced RPMs and radiography systems.

Mr. Chairman, this concludes my prepared remarks, and I look forward to your questions.

Senator COLEMAN. Thank you very much, Mr. Oxford. Mr. Ahern.

TESTIMONY OF JAYSON P. AHERN,[1] ASSISTANT COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION

Mr. AHERN. Good morning, Mr. Chairman, and thank you for the opportunity to be here today. I'm pleased to join my colleagues from DNDO as well as NNSA to discuss an issue of prime importance to Customs and Border Protection and to the security of our Nation, and that is preventing the smuggling of nuclear and radiological weapons into the United States.

Mr. Chairman, CBP's priority mission is homeland security, keeping terrorists and their weapons, including weapons of mass destruction, from getting into our country. That means improving security at our physical borders and ports of entry. And it means extending our zone of security beyond our physical borders so that America's ports of entry are not the first line of defense against the international threat of terror.

After September 11, CBP developed and implemented unprecedented initiatives, all driven by the understanding that the threat still exists and is still very real, and that CBP must and will do everything humanly possible to prevent a second attack.

In assessing how far we've come in setting in place the mechanisms that protect our country from terrorist attack, I believe it's

[1] The prepared statement of Mr. Ahern appears in the Appendix on page 173.

worth noting that before September 11, there was not a 24-hour Rule or Trade Act requiring advanced information to be transmitted prior to shipment to the United States. Before September 11, there were no National Targeting Center, where multiple Federal agencies worked together to identify both trade and people of risk.

Before September 11, there were no CBP officers working together with our counterparts in foreign countries to identify and screen high risk shipments before they're bound for the United States. And before September 11, there were no concerted public and private sector partnership against terrorism, working to improve the security and the efficiency of trade. And before September 11, there was no radiation portal monitors at our ports to screen cargo containers. And there were only 16 large-scale x-ray devices in use at our U.S. seaports.

There is no question that our Nation's 322 ports of entry today are far safer than they were before September 11. But at the same time, we're all aware that securing our ports and the global supply chain is work in progress, and we must do more.

I'd like to spend the remainder of my time responding to your letter of March 8, specifically and very candidly to the concerns you outlined in your letter of invitation.

To begin with, first, the subject of this hearing, and that's detection technology. I'm able to report that CBP does currently operate 740 radiation portal monitors at our Nation's ports of entry, including 190 at our seaports. And RPMs today are our most robust radiation detection equipment, allowing us to quickly and thoroughly screen for radiation.

In addition to the large-scale technology, CBP has deployed 491 radiation isotope identifier devices and 12,500 personal radiation detectors. And overall, the RPMs that we currently have deployed on the northern and southern border and to date at our seaports, 67 percent of all arriving land and sea containerized cargo coming into the United States is run through the radiation portal monitors. By the end of next year, 2007, we'll have 621 RPMs deployed at our Nation's top sea ports, giving us the ability to screen 98 percent of inbound sea containers.

Beginning next month, CBP will also begin to deploy 60 mobile RPM systems at our seaports, and these mobile rpms will give us the flexibility to screen low volume locations as well as real-time screening of high risk containers shipside. We expect these RPMs, these mobile RPMs, to be in place by the end of this year.

To date, we have also screened over 80 million containers with RPMs, and we've resolved over 318,000 radiation alarms. We have resolved all the alarms, and the majority of the alarms have been attributed to naturally occurring radioactive materials, known as NORMs, and no alarms have been attributed to illegal nuclear material coming into this country.

I would like to briefly comment about the GAO red team testing, and that is the attempt of GAO to introduce, smuggle into the United States, radioactive materials through two ports of entry on the northern and the southern border.

I believe this was a very good opportunity for us to test our systems and our protocols in a real life situation. Although our sys-

tems worked, and our officers appeared to have followed our protocols for radiological alarms, the bottom line is the material was allowed in with questionable documentation.

We have learned, and we're working to strengthen our protocols immediately so this does not happen again. We agree with GAO's assessment, and we assure that we are working with all their recommendations, but particularly on establishing a process for validating NRC licenses, and we expect to have a process in place within 30 days.

For the container security initiative, it's important also to mention that we've made enormous progress, pushing our borders out. As of this morning, just this past Saturday in Honduras, the Container Security Initiative is now operational in 44 ports, the most recent in Puerto Cortes, and recently before that, on March 8, in Port Salalah, Oman.

Since 2002, CSI, we've added at least one port a month to the program. And these 44 ports currently amount for—75 percent of the maritime cargo containers coming into the United States to have an opportunity to be screened for risk. By the end of 2007, we'll have officers stationed at 58 ports, totaling 85 percent of the container traffic coming to this country.

I'm also proud of our partnership that we have with the private sector under the Customs-Trade Partnership Against Terrorism. And today C–TPAT has nearly 6,000 certified partners from the private sector, including some of the largest U.S. importers, working to increase supply chain security from foreign loading docks to the U.S. port of arrival. Through C–TPAT, CBP reviews the security practices of companies shipping goods to the United States.

A year ago we had only 8 percent of the certified members validated. Today we have 27 percent done, and we have another 39 percent underway, so that we'll be at 66 percent by the end of this fiscal year.

I know there's also been concerns about the number of validators we have on board, supply chain security specialists. Today we have 88 on board; within the last 2 weeks we have selected 41 additional validators, and they'll be on within the next 30 to 45 days so that they're on board for a May 15 training class. And by the end of the summer, we'll be at our 156 target.

I also would like to talk to you about an additional protocol that we've put in place. We have recently entered into an agreement with 19 recently retired Customs and Border Protection officers and special agents from Immigration and Customs Enforcement to have them involved and trained, given the exact same training as our supply chain security officers, so that they can use their experience in offsetting our teams to increase the pace of validation overseas.

With regard to our targeting systems, CBP, our partners within the government, we're also looking to increase the targeting capabilities at the National Targeting Center. Certainly we look to continue to improve the integration of our intelligence through our targeting efforts and the data elements we need to make our system more comprehensive and accurate.

Recently MitreTech Systems, an independent consulting firm, performed an independent evaluation of CBP's Automated Tar-

geting System and targeting methodology. CBP uses ATS to identify ocean containers that are high risk for terrorism. The assessment identified a number of strengths, including recognizing our assets of how highly trained our officers are.

They also recognized our ability to adjust rules and weights to account for priorities, risk, and changes. But they also made a number of recommendations, such as the ability to have an infrastructure in place to test the simulation of proposed rules or mock shipments, and we continue to improve under their direction.

Last, under the Hong Kong ICIS program, I believe it's important just to offer my comments in addition to Mr. Oxford's. I've had the opportunity to see this concept, and certainly it employs technology that integrates into a single computer screen the radiation profile and VACIS image, much of the same technology we use at our ports today.

But I believe today the Hong Kong concept is just that, a concept, and the effectiveness of this concept has been overstated. But nevertheless, it is consistent with our strategy to push the borders out, and I believe it does have the ability to complement our CSI program. And we're committed to partner with the private sector to develop a viable concept of operations. And this will take also a considerable amount of support from the host country counterparts as well in each country we would go to.

In conclusion, we know that securing America's borders is an ongoing and long-term effort, but we can be proud of what we've been able to accomplish thus far, and to make America safer and our seaports more secure.

Mr. Chairman, we welcome the oversight of this Subcommittee and you personally, and suggestions our colleagues at GAO as well as independent reviewers like MitreTech have made to improve our programs. We take these recommendations very seriously, and work every day to improve the ways we carry out our homeland security mission and to keep terrorists and terrorist weapons, including weapons of mass destruction, nuclear, and radiological weapons, out of our country.

Thank you for the invitation today, and I'll look forward to taking any questions later.

Senator COLEMAN. Thank you very much, Mr. Ahern.

I want to start by acknowledging the clearly substantial improvements from where we were on September 11. Today, we have the National Targeting Center, C–TPAT, CSI, and we are utilizing radiation portal monitors. So there is no question that we're safer today than on September 11.

However, are we safe enough? Have we elevated this issue to the highest priority and are we responding accordingly? As I said to Secretary Chertoff when he was being confirmed, unlike perhaps any other department head, if the head of transportation—if there are highway deaths on the highway, it's part of the reality of the world we live in, and you don't get a lot of feedback. And if there are environmental spills, we deal with that; a great concern, but it's the world we live in. But in this area, failure's not an option. And so the standard is higher, and in part, that's why we've been so vigorous in this oversight.

I just want to, if I can, talk about ICIS for a second. And I appreciate the fact that we're hearing that it may serve as a model. I was in Hong Kong and I saw the ICIS system. I also appreciate the recognition of working with the private sector and with foreign entities. I think as a result of some of the concerns about the DP World process, about whether it should have had a 45-day review, I believe; the law required that, it didn't—but I don't know if we ever got to the substance.

And part of the reality is that if our defense requires us to work vigorous, requires us to work with foreign entities in some capacity, we do that. We have to take a close look at it. But I appreciate the recognition that this is part of the reality.

My concern about ICIS is I hope we push the envelope. Clearly, and I think, Mr. Oxford, your comment, it's a model. It's not an operational system. The fact that you can do a couple lines—and I was there. Every truck rolls through. It doesn't stop. It doesn't interrupt the flow of commerce. You've got the image. You can check that, then, with a manifest. You tie that in with the radiation portal monitor.

We then have a couple-week period while containers are coming over here and perhaps subject to further analysis, which I think has been the issue. I've got to believe that with computer technology, we'll be able to do some analysis which will give us more information.

But I'm hopeful that we're taking a close look, and that there isn't any kind of bureaucratic resistance.

Let me, if I can, talk about Megaports, and then I want to talk a little with you, Mr. Ahern, about ATS and about our targeting system. There's been a lot of discussion publicly about Megaports deployment in the Bahamas, and with Hutchison Port Holdings awarded a sole source contract. They operate the port in the Bahamas, don't they?

Mr. HUIZENGA. That's correct.

Senator COLEMAN. So if you want to operate in the Bahamas, you're going to give a sole contract.

Mr. HUIZENGA. They're the only people driving those vehicles around on their port.

Senator COLEMAN. And I would take it that it's your judgment that it is in the best interests of this country to have a Megaports program, to be working with folks like Hutchison and others to make sure that we're putting in that extra line of defense.

Mr. HUIZENGA. Absolutely. I mean, pushing the boundaries out is what this is all about. And it's important to note that we reviewed our relationship with Hutchison before we started to pursue the contract, and we're convinced that they're a company worth working with.

Senator COLEMAN. I worry there's a little bit of xenophobia here. However, I believe that if foreign countries are operating ports, then they should establish an American subsidiary.

Foreign companies operate 80 percent of our ports. It is a reality at today's world for the U.S. Government to work with foreign companies. Yet I hope we will take a close look, and understand what the gaps or concerns may be. I am certainly one who believes that

Megaports is part of this integrated infrastructure and I hope we continue moving forward.

Can I just clear something up about numbers? We have good coverage of our southern and northern borders, somewhere in the 90 percent. I thought it was stated that we'd have 98 percent of our containers coming in from ports.

Screened for radiation by 2007? Is that correct? The question I have is, however, when do you have "full coverage"? GAO says not by 2016. I thought the Secretary said by 2009. Can you help me understand the difference? Are we committed to this accelerated process that would make the GAO number somehow not relevant based on what we intend to do over the next couple of years?

Mr. AHERN. Yes. I would tell you that our projection right now for the RPMs for seaports would get us to 621 RPMs by 2007, and that would get us to 98 percent of the sea containers coming in through the top 22 ports.

Senator COLEMAN. Senator Levin is not here, but there was a comment about imaging technology. It may have been you, Mr. Oxford, who discussed some of the capabilities of the new technology. That chart is a scan of a truck carrying garbage from Canada into the United States.[1]

And perhaps any of you gentlemen can help me. Even with all the technology that we have today—you talked about imaging systems, high density cargo. I presume that's high density cargo right there. How do you know whether there is a dirty bomb buried in there? How do you know whether they've got any kind of weapon of mass destruction? How do we somehow stop that from being a carrier for some weapon of mass destruction?

Mr. OXFORD. Mr. Chairman, that's why when we looked at the ICIS system, we look at some of the operational and technical limitations. The VACIS system originally was designed to look at contraband and other anomalies for customs' other missions. What we're looking for in next generation radiography systems is to actually have better information content, where we can now discriminate between the material that's in that cargo.

So it's not just the ability to find high density material. It's to identify the differences in density so we can look at those anomalies and red flag for the operator the material in that cargo that you care about. So what you're seeing on this image is a current generation capability that has very little information content and requires a lot of operational judgment.

Senator COLEMAN. Mr. Ahern, the basis for our system today is really—the Automated Targeting System. And in terms of what we inspect, do we have the chart that shows the various ports, the foreign ports? I think it says Le Havre and some others.[1] Is there a chart there that says these are the number of high risk cargos? These are the numbers of requests that have been made to actually do a screening. I think that's the one.

A couple of questions. We've got CSI ports, Container Security Initiative. And by the way, where they work well, at least in Hong

[1] See Exhibit 15 which appears in the Appendix on page 440.
[1] See Exhibit 7 which appears in the Appendix on page 371.

Kong, our folks are operating side by side. Is that the model throughout all the CSI ports?

Mr. AHERN. We do find that Hong Kong is one of our better footprints for our officers working alongside. We do have that in many other locations as well.

Senator COLEMAN. But we don't have it in all the locations?

Mr. AHERN. The side by side officers?

Senator COLEMAN. Yes.

Mr. AHERN. Not in every location.

Senator COLEMAN. I mean, to me it is important to work side by side. In Hong Kong, I saw how well that operated. There must be things we can do to somehow facilitate getting folks to work side by side.

But one of the questions I have is if you look at the green, the green are the high risk shipments. Now, I presume high risk, is that through an ATS targeting system?

Mr. AHERN. Yes. That would be.

Senator COLEMAN. And then we go to the country and we go to Hong Kong, and you can kind of see. And even with my Lasik vision here, I can't look at it exactly. But what you have is 37.2 percent of high risk shipments are examined at Hong Kong. And we actually have a higher number that are requested. And that decision to actually examine is done then by the host country. Is that correct?

Mr. AHERN. That is correct.

Senator COLEMAN. Even with this system, we don't control whether it's examined there. Now, those that we've asked—the yellow that we've asked to be examined—forget the green in which there are lots of high risk. But those between—those we've asked to examine in the yellow, do we examine those containers then before they're actually unloaded on our shores?

Mr. AHERN. If they're determined for high risk, they would be examined upon arrival in the United States if they're not done overseas.

Senator COLEMAN. What about all the high risk that are not inspected? In regard to Hong Kong, 15,636 are identified high risk; only 5,580 are actually examined. What about those 10,000? Are they also examined here?

Mr. AHERN. Those would be examined in the United States.

Senator COLEMAN. In what way are they examined?

Mr. AHERN. They would be given as far as the radiation screening as well as the NII, physical examination, if necessary.

Senator COLEMAN. Physical—when you say if necessary, out of those other 10,000, how many are actually physically examined?

Mr. AHERN. I would have to give you the precise breakout.

Senator COLEMAN. Can you give me a ballpark figure?

Mr. AHERN. I wouldn't want to provide a speculative answer.

Senator COLEMAN. If you look at Le Havre, France, what you have here is 1,649 identified as high risk. You only have 244 actually examined there, 553 not. So the French authorities simply made a decision that over half those that we request to be examined aren't examined. Is that correct?

Mr. AHERN. What I'd like to do, if I might, is I know that taking a look at the snapshots in time that were used from this, February

2005 to February 2006, I know in the early part of 2005 that we were not getting the responsiveness that we had hoped for in Japan and in France. So if I might, if I could actually provide some more detail after this hearing to show the progress that has been made in recent months to bring those numbers to adjust those bars a little bit more positively.

Senator COLEMAN. I'd appreciate it. Because clearly what we would like to see is, we'd like to understand, if there's resistance from the host country, what are we doing to change that? What kind of tools can we use to say, we have a concern, and if this is really a partnership, we need you to act a little more aggressively. Because it seems to be somewhat varied in terms of the nature of the response. And actually if something is high risk and we want it to be checked, you would expect we wouldn't want to have any variance.

Mr. AHERN. Absolutely. And I think we can provide some information as a follow-up to this hearing to show what it's been in recent months, moving towards the goals that we would like.

Senator COLEMAN. Let me focus on ATS for a second because it really is kind of at the root of our system, what we identify, and we'll get into all the details here. But we essentially, through a range of factors, give cargo a rating, and based on that rating we make a determination as to whether it's high risk and then once that determination is made, we will then determine whether in fact there's some extra review accessory.

The system itself, have we ever conducted any kind of peer review? Have we ever done any kind of analysis that substantiates the veracity, the accuracy, of this system?

Mr. AHERN. Yes. That was the MitreTech review that I spoke of in my short statement. That outside review actually pointed to a lot of things that we had that were strengths of the program as well as additional areas we needed to improve upon.

Senator COLEMAN. Do you ever do any red team testing where the system is actually checked it out. Do you do simulated testing? Have you ever gone down there and seen whether you could escape and get through this system that we place such reliance on?

Mr. AHERN. With, again, the MitreTech study that was done, we have now some protocols that we're going to begin to operate within the next month to 2 months to start—do some what they call in the sandbox testing for us.

Senator COLEMAN. So we're going to do that now?

Mr. AHERN. Yes.

Senator COLEMAN. OK. And I hope we do that now. I mean, again, this is the kind of underlying basis or—we're banking everything on a system that we've done some studies. We have not done the kind of testing that says, OK, is it vulnerable? Does it work?

And if it does—and I applaud, by the way, Customs and Border Protection and DHS, in regard to what we saw with the radiological material—which is interesting, by the way. I did read in the paper they said we'd have that document problem fixed in 45 days. I do know your testimony today says 30 days. So I'm going to hold you to the 30 days.

Mr. AHERN. Fair enough.

Senator COLEMAN. But I do appreciate it. But I think we—again, we need to take a look at this.

My other concern is simply the reality that this is a sampling. It's not random. It's targeted.

Mr. AHERN. Right.

Senator COLEMAN. It's a targeting system, but that depends on C–TPAT and other programs. You've got relationship with shippers and companies like Best Buy, etc., that we put a lot of stock in what they're doing without the kind of thorough review investigation.

And so in effect, you've got a lot of folks who are going to have a pass. And I think that was in Commander Flynn's scenario. They're going to get a pass on any kind of high risk based on getting points for relationships that I worry where someone could understand that and use that as a way to break through that system. That's one of the vulnerabilities we have. Is that correct?

Mr. AHERN. Well, what I would just add to that is that without getting into too much of our scoring in an open hearing like this, I would remind all of us of the change in protocols that we had going back several months ago where we actually did cease providing any kind of an advantage at the time of manifest filing when we do the initial scoring. And there's not any at that point in time for the security screening that goes that 24 hour prior to lading.

Senator COLEMAN. But the problem even with that is that we look at a company and we give it certain credit. But we're really not looking at all their operations. We're not out there checking to see whether in fact what we believe to be their system—we may have looked at one place, but there's not a uniform review, certification process that gives us—certainly not 100 percent certainty. In fact, I think it's a lot less than that. But, I mean, that is the system we have.

Mr. AHERN. Well, if you're talking about the validations, we have a very uniform way of going out and doing the validations now. It's much more consistent than it was, again, even just several months ago. That's, again, lessons learned from a previous GAO report.

Senator COLEMAN. Mr. Oxford—let me just finish, if I can, with ICIS because one of the benefits of ICIS is at least we could have the images of the containers in this chart. Today, we don't have images for those containers in Hong Kong.[1] Again, this chart is dated, a moment in time.

But right now we have a system that says of the 15,636 high risk shipments examined at Hong Kong, we know that 5,823 are actually checked there. We've identified 7,918 that we'd like to be checked. We do believe that before they get in, those are covered. I still have a question as to the 8,000 to 10,000 spread which we've identified high risk, whether in fact those are checked before they get here and what that means.

But at least with ICIS, just using that as part of a system, we'd at least have a screen. We'd have an image. We'd have a manifest. We'd have a radiation portal monitoring of all these high risk, which we don't have today. Is that correct?

[1] See Exhibit 7 which appears in the Appendix on page 371.

Mr. AHERN. That would. And just to put ICIS in its proper context as we go forward into the future, I think it is appropriate to take a look at. It's very consistent with our pushing the border strategy out, and it would be very complimentary to the 44 ports where we currently have CSI.

And when our targeters overseas would get a score for risk, one of the first things they should then ask for is, let me have the electronic file that is there for this container coming in so they can again make an informed decision of what's going on.

But it won't all just be through that protocol. There will certainly be a lot of alarms that will be occurring. As I stated, with the 80 million containers that we've now put through the RPMs, 318,000 have resulted in alarms that needed to be resolved. And I would submit to you, and I know there's been a lot of discussion by many who've looked at this issue, and I would think that the carriers would support the same position that I'm going to proffer at this point, any alarm needs to be resolved before it's put on a vessel for the United States.

Anything using it for forensic capabilities en route or after route within the United States may be interesting to have, but you would want to make sure that the alarm is resolved before it's put on a vessel for the United States so that there's not any concern about something happening en route or upon arrival. So that would be a very critical component that needs to be added into this process.

Senator COLEMAN. Mr. Oxford, last line of questioning. I believe you were quoted in one of the articles today talking about the red team testing that GAO did and the material that at least set off a radiation portal monitor. So the monitors were set off. Clearly, from a monitoring perspective, there was enough material in there to raise the level of concern. Is that correct?

Mr. OXFORD. Yes.

Senator COLEMAN. And GAO says that based on their analysis and working with a couple of other government agencies, they thought this was enough to make dirty bombs. Is that correct?

Mr. OXFORD. That's what they said, yes.

Senator COLEMAN. And your comment was it was somewhat minimal material.

My question is this, though—two questions, actually. One, you're not discounting the impact of dirty bombs, are you?

Mr. OXFORD. Absolutely not.

Senator COLEMAN. And so the testimony of Governor Kean in terms of the emotional impact, or Commander Flynn in terms of the economic impact, you wouldn't disagree with that, would you?

Mr. OXFORD. Not at all. In fact, when you look at our Securing the Cities Initiative, we were going to focus a lot in the urban areas on a dirty bomb-like attack, and what we can do to prevent and immediately mitigate those effects.

Senator COLEMAN. And the other concern that I had in this regard is, again, without debating how much material was in those two boxes, it was the sense from GAO that they could have gotten a lot more material without raising any red flags. What do we have to put in place to make sure that there are red flags so that people can't get radiological material in a level enough to build a dirty bomb without anybody being concerned about it?

Mr. OXFORD. Well, even though that falls mainly in the domain of the Nuclear Regulatory Commission, I think the exercises and the ability for CBP to do what they're proposing to do, especially for the cross-border activities, certainly allows an extra layer of security to be able to look at that material.

It was mentioned in the opening statements that the Energy Policy Act that dictated NRC lead a task force, with a report due to Congress this August, I think we, as a government, need to look hard at the recommendations that come through that process to make sure we're all doing more for source security within the country as well.

Senator COLEMAN. Let me ask the last question then about a general concern. We've got a lot of agencies involved in this effect. What we had, if you look to that Second Line of Defense program, we have a question about whether the State Department—the records they had in terms of the devices and everything else. We have DOE now. We have Homeland Security. I think there may be some other entities.

Is there a concern that there are too many cooks cooking this broth, and that perhaps we need to somehow better centralize this? Is there going to be a concern, if something goes wrong, that a lot of people are going to be pointing fingers and say, there wasn't a single person in charge? Because we've been through that dance before. Anybody want to respond to that?

Mr. OXFORD. Mr. Chairman, if I could try to take that on because I may be one of those people they point at when that time comes.

We have seen within the 11-plus months that we've been in existence that we have a daily dialogue now across the inter-agency that didn't exist on a routine basis in the past. We think that was one of the preeminent reasons for why DNDO was created, was to create that daily dialogue.

It does not mean we have to run every program. And we're seeing the benefits from having the NNSA people on our staff. Mr. Ahern has 11 people from CBP within the DNDO office. It's creating this dialogue on a daily basis. And that extends to the Department of Defense, the Department of State, the Federal Bureau of Investigation, and now we have two NRC people on the staff to start working these issues.

So I think we're making a great step forward in creating that cross-talk that was necessary in the past.

Senator COLEMAN. I appreciate that. And I would just urge that if there's even any inkling among you or folks who work with you, any of the other agencies, that somehow we're seeing the beginning of some silo effect where people are questioning the level of communication and cooperation, I would hope that is attended to very quickly because were that to happen, I think it would be very problematic.

Mr. HUIZENGA. Mr. Chairman, I'd like to echo Vayl's point. I really believe we have a significant amount of communication right now, and it benefits us because we're able to bring the expertise from the different agencies to bear on this common problem.

And, we can share the expertise that we've developed over the last decade working in foreign countries, and we can help on the CBP's efforts with CSI in order to provide that additional layer of

radiation detection screening before the containers leave the foreign ports.

Senator COLEMAN. I thank you. We will have a hearing on Thursday. We'll focus more on ICIS, focus more on C–TPAT and CSI. But this has been very helpful, and I do thank you for your testimony.

With that, this hearing is now adjourned.

[Whereupon, at 12:25 p.m., the Subcommittee was adjourned.]

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

THURSDAY, MARCH 30, 2006

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Norm Coleman, Chairman of the Subcommittee, presiding.

Present: Senators Coleman and Levin.

Staff present: Raymond V. Shepherd, III, Staff Director and Chief Counsel; Brian M. White, Professional Staff Member; Joanna Ip Durie, Detailee, ICE; Mary D. Robertson, Chief Clerk, PSI; Leland B. Erickson, Counsel; Mark L. Greenblatt, Counsel; Steven A. Groves, Counsel; Cindy Barnes, Detailee, GAO; Elise J. Bean, Staff Director/Chief Counsel to the Minority; Laura Stuber, Counsel to the Minority; Hanni Itah, Intern; Kathy Kraninger (HSGAC, Collins); and Henry Abeyta (Energy, Domenici).

Senator COLEMAN. This hearing of the Permanent Subcommittee on Investigations is called to order.

I know that Senator Schumer is on his way. I am very pleased to see my good friend and close colleague, Senator Graham, here today. Both Senator Graham and Senator Schumer have really taken a lead on this issue of container security, and have recently visited Hong Kong. As part of our discussion today, we will be talking about the ability to screen 100 percent of containers and an operation in Hong Kong. Both Senator Graham and Senator Schumer, have just returned from Hong Kong and I thought it would be very worthwhile for this Subcommittee to hear from them abut their trip.

Senator Graham, I am going to turn it over to you before my opening statement. I anticipate Senator Schumer should arrive shortly. If he is not here, I will give my statement, but I would like to give you the opportunity to begin first. I know both of you are busy.

I welcome the Ranking Member. Senator Levin, I indicated that I was going to give both Senator Graham and Senator Schumer the opportunity to talk a little bit about their experience before our opening statements.

Senator LEVIN. That is fine.

Senator COLEMAN. I know they have to go on their way.

Senator Schumer is finally here, and I am very pleased to see him. I also indicated that both of our colleagues have taken a very strong interest in the whole issue of port security, container security, and personally visited Hong Kong recently to look at one of the systems there.

Senator Schumer, what I am going to do is I am going to have you and Senator Graham speak before we do our opening statements. As soon as you are done—I know that you are in the middle of markups and other things, we will certainly excuse you at that time, but I do want to thank you for being here today.

With that, Senator Graham.

TESTIMONY OF HON. LINDSEY GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Senator GRAHAM. Thank you, Mr. Chairman. You are right, we just returned from Hong Kong and China, the Mainland, and my body is somewhere between there and here, so I will try to make this brief and to the point.

In terms of leadership, I know Senator Schumer has been talking about port security for a long time, and Senator Levin has been talking about national security matters every time we meet, in Armed Services he is talking about these things. Mr. Chairman, your bill is sort of a model, and that is how I got involved, by talking with you and the gentleman from Hutchison behind us. You kind of set us up.

I have Charleston port in South Carolina, and we are looking at locating a new port. I guess the Dubai Port World experience has sort of woken up the country a bit, and let us take advantage of what was an unfortunate event, but it did tap into some concern out there about how our ports are operated, who should own the terminals and are we where we need to be as a Nation? In that regard, the whole experience could be positive. Senator Coleman, I want to be a partner with you and Senator Schumer, and Senator Levin, and others to try to get this right.

The Hong Kong experience was very exciting. We met with the Hutchison people, and we viewed a system called ICIS. I think you have already been there. One of the things we have learned from this whole Dubai experience, that most Americans did not realize that most of the cargo coming into our country is coming in basically uninspected. We have a screening program of sorts, but the technology to look into each cargo container and find out if it is something we want or something dangerous to us as a Nation seems to be developing rapidly. The only thing not developing rapidly is our government's ability to deal with port security. Maybe from this whole episode and your bill, and other pieces of legislation, the government can catch up to the private sector.

Here is what was so exciting, is that the technology that Senator Schumer and I had the pleasure of viewing, seems not only to be technically good, but commercially sound, that you can screen cargo at the biggest port in the world without bringing our commerce to a halt. What we are lacking is infrastructure within out government to take those images and analyze them to make sure that the

container does not carry contraband or weapons of mass destruction or other things that would hurt Americans.

As a Nation, I believe it will be political malpractice for us not to come together as Republicans and Democrats and put the infrastructure in place to take this promising technology and spread it worldwide. We can do it in partnership with the private sector. That was what was so exciting. This is not another government program of many layers. This is allowing us to tap into private sector innovation where we could partner with the private sector, let them lead the way in screening and inspection, and we will have some infrastructure in place at the Federal level to make sure we know the results of these screens, to make sure the cargo is safe to come into our country.

One final thought. This has to be done worldwide, and it has to be done with the private sector taking the lead, and we are trying to do it with other nations. The Bahamas event is sort of the wrong model. No one in the United States wants to take over the sovereignty of the Bahamian Government or any other government. We want a partnership, sort of like we have with airlines, where governments can work in collaboration with our government and the private sector, to make sure that commerce is secure for us all, because if there is a terrorist attack on our shipping lanes or at any port in the United States, or any major port, the ripple effect would be devastating to the world at large. So we have a chance to collaborate with nations that have ports with their borders, and make this a win-win.

That is what I am looking for, a marriage between the private sector, our government and the world at large, to make sure that we know what is coming to our shores, because the one thing I have learned from this whole episode, after talking with you and others, Mr. Chairman, is this is probably the weak link in the national security chain. The good news: We can solve the problem if we work together and we get ahead of it.

With that, I appreciate the opportunity to be before your Subcommittee, and look forward to working with you and others to solve the problem.

Senator COLEMAN. Thank you, Senator Graham. In your time in Congress, both in the House and here, you have been a champion on national security issues. I greatly appreciate you bringing your passion, your intellect, and certainly one thing the good Lord gave you in much bounty, and that is good common sense, bringing it to this discussion. It is much appreciated, and I look forward to partnering with you.

Senator Schumer.

TESTIMONY OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Thank you, Mr. Chairman. I want to thank you for your leadership on this issue. Just the report that was issued the other day should be a wake-up call to everybody through your Committee, your Subcommittee. I want to thank, of course, my good friend, Carl Levin, for his leadership as well.

This is an issue whose time is due, and the whole whirlwind about the Dubai Ports can have some good, and the good is that

we really do tighten up port security, and the good news, I think all of us are aware, and particularly Lindsey and I on our visit to Hong Kong, is that it can be done. It can be done without impeding commerce, and it can be done without much government expense, and this is all very good news.

First let me say our trip to the Hutchison Whampoa Terminal in Hong Kong just knocked my socks off. First, it is as large as could be. I thought we had big ports in New York, but they are dwarfed compared to the Hong Kong port in size, but also in terms of efficiency and modernity and so many different ways.

But second, their system of security, of checking each container, not 5 percent, not 10 percent, not 50 percent, but 100 percent of all the containers, for nuclear and other detrimental materials is just incredible, and they do it without slowing down commerce at all. In fact, our Customs people told us their biggest problem is that the containers are checked so quickly, that sometimes they have a rough time catching up with them because they are already at sea by the time they get information on the check. That is something that has to change, but it is an easily solvable problem.

I have not seen anything in the United States—and I have studied port security that compares to what we saw in Hong Kong, and that is a shame. It is a shame that China and Hong Kong could have better port security than we here in the United States, and the system that we have seen—and I know you have been enthusiastic about and champion, Mr. Chairman—should be our standard.

As you know, they first create an image of every container's content that can be sent and reviewed by Customs officials in real and near-real time to ensure not only what is in there, but that if there is, say, a lead box that might contain something that is bad, they will come up with that, too. That has always been my great worry since I introduced legislation years ago to require scanning of containers for nuclear materials. The way they figured this out is they have three different check levels, and when the three match up, you know something is wrong and you pull the container. And maybe in that lead container or that imperceivable container will be nothing bad. Well, so be it. Better to be safe than sorry.

The other bit of good news is the cost is amazingly low. It costs, I learned on our trip, about $2,000 to send a container from Hong Kong to the United States. That, by the way, is very cheap as well. It is one of the reasons we have so much more commerce, because this man, whose name I forget—sounds like—McLean. Mr. McLean, who developed these containers really did the world a service. So it costs only $2,000 to send a container across the ocean, Pacific Ocean. It is probably a little less for the Atlantic. Guess how much it costs to do this? About $6.50. Now maybe it will be a little more in ports that are less efficient. Hong Kong is the world's largest port. Let's say it is $20. One percent, adding $20 to the cost of a $2,000 container to make sure that it does not contain material that might be terribly dangerous to us, makes eminent sense.

So what I think—and I know I have talked to you, Mr. Chairman, Senator Graham, some of the others—we could mandate this on every container that comes into the United States, mandate a system like this be used. Could not do it immediately, but over a

reasonable period of time. The technology could be adapted to each port. We saw how they are adopting it in Bermuda, where they would not have a long line like this, but they actually have a truck where the detectors go by the containers instead of the containers go through a sort of toll booth. It would not cost the government a nickel.

Now, there would be some government costs, because the scanning is done here in the United States. You just send it by broadband, somebody sitting in a Customs office, maybe in New York City—that might be a good location for such an office——

Senator GRAHAM. Or in Charleston. [Laughter.]

Senator SCHUMER. But somewhere in the United States could just scan this with the expertise, send the OK right back. Broadband allows us to do things that were unimaginable 10 years ago. So we would have to hire some more Customs inspectors, but when you think of all the people we see at the airports who are government employees, this is a small cost for port security, which is much wider open than air security.

So the work of this company, Hutchison Whampoa, which is the largest port operator in the world, has proved DHS wrong. This can be done. It is an example of what should be done in the private sector, and we should be as aggressive as they are in making sure that everything is screened, and require it to do it.

My nightmare, Mr. Chairman, has been, ever since September 11, that somebody somehow smuggles a nuclear weapon into one of our cities, not just a dirty bomb, but a real nuclear weapon. If, God forbid, that were to happen, there would be enormous loss of life, the economy would be disrupted, and our whole way of life would probably change, the wonderful way of life we have here in America. It is worth a little extra effort and a few extra dollars to make sure that does not happen.

I look forward to working with you, Senator Levin, Senator Graham, to make that a reality as soon as possible.

Senator COLEMAN. I do not know if there has been a more zealous and passionate advocate for this kind of security than you, and for obvious reasons, representing New York State, representing the World Trade Center area, and I know a very personal loss to you. I appreciate your continued passion and focus, and look forward to working with you.

Senator I am going to excuse our colleagues. Senator Levin, anything you want to add?

Senator LEVIN. I just want to thank both Senator Graham and Senator Schumer for all they have done in the Senate, most recently for their trip to China. It was very important to all of us that you raised the issues that you did with the Chinese about currency manipulation—that was the one we followed the most closely—but also for your taking the time then to go to Hong Kong and to inspect that technology.

I know our Chairman has done the same thing, so we have a Chairman who is on the job on this issue, and I am going to be working with him, and look forward to working with both of you.

I would just make one point, which is not directly, perhaps, related to the technology issue, but as the Chairman and I both know, 11 million containers come in by sea, but 11 million con-

tainers come in by truck, and so this technology is critically important to all border States, not just to States that have ports, and in addition, we have a couple of million containers by train which come in. So this involves the safety of all Americans, but directly involves many more States than just the States that have seaports.

Senator COLEMAN. Colleagues, thank you.

Senator SCHUMER. I would just say, just from my look there, it seems to me that the technology could easily be adopted for land and train as well as port, and we would have to do that, because terrorists look for our weakest pressure point.

Senator GRAHAM. Mr. Chairman, if I may add, this trip was everything you said it would be. That is what got me to go to the port, is through our conversation you suggested while we are over there. It was, as Senator Schumer said, astounding what the private sector is doing.

And one brief commercial for South Carolina. There is a program called Project Seahawk that has been in the budget now for 3 years that Senator Hollings started. We have 40 different law enforcement agencies at the Federal, State and local level, working out of one building in Charleston, South Carolina, sharing information about port security by turning to their left or to their right, to talk to people. My goal is to make sure that program thrives and survives, and everybody in the country can duplicate this model of talking to each other at every level of government. It would add a lot of security to our ports and other places.

Thank you for what you are doing, it is very important.

Senator COLEMAN. I thank you for your leadership, and I look forward to working with you. Thank you very much.

OPENING STATEMENT BY SENATOR COLEMAN

Senator COLEMAN. Today we will conclude our two-part hearing on neutralizing the nuclear and radiological threat and securing the global supply chain. On Tuesday, we extensively discussed the threat of nuclear or radiological terrorism. The consensus was clear: The threat is real and we are not doing enough to prevent it.

Commander Flynn, who testified before us on Tuesday specifically outlined a stark scenario of a dirty bomb transported to the United States via a maritime container. However, this is not simply a worse-case scenario. One of our witnesses today will testify how 2 years ago, Palestinian suicide terrorists evaded port security in Ashdod after being smuggled in a secret compartment within a container from Gaza. Ten Israelis were killed and 16 others wounded after they intercepted the terrorist before they reached their target. It is suspected that the suicide bombers were intending to blow themselves up near the tanks of hazardous material after inspectors found unexploded grenades within the secret compartment.

Experts in the industry believe it is just a matter of time before terrorists break security measures at a port of entry, most likely with a dirty bomb. These hearings are designed to prevent that from happening.

Global trade is one of the pillars of our Nation's economy. American national security is inexorably linked to economic security. Governments across the world must ensure that the supply chain

is secure, but must also do so without impeding the flow of commerce. More than 90 percent of global trade moves in ocean-going containers, and over 10 million containers enter the United States annually.

The Congressional Budget Office, at my request, studied the economic consequences of an attack on the Ports of Los Angeles and Long Beach.[1] CBO found our Nation's gross domestic product would decline by about $150 million per day for each day these two ports are closed, and that the annual cost of closing these ports would escalate to nearly $70 billion. While CBO did not analyze the cost to human life and property of such a terrorist attack, the economic impact of closing the ports could be comparable to both the attacks of September 11 and Hurricane Katrina. We cannot afford the devastation these findings imply. We must secure our supply chain before we pay the high price of an attack, and seek the appropriate balance between two often-competing priorities: Security and speed.

Former Customs and Border Protection Commissioner Bonner had the vision to address this grave threat and balance these two priorities—security and speed—after the September 11 attacks. This balancing act resulted in the creation of two of the most prominent Homeland Security programs—the Container Security Initiative (CSI), and the Customs-Trade Partnership Against Terrorism, or C–TPAT. CSI effectively pushed our borders out by placing CBP officers in foreign ports to inspect containers before they reach our shores. C–TPAT exemplified a true public/private partnership.

These ideas alone are laudable—but due to the sheer magnitude of the challenge of securing the global supply chain, we must continue to improve upon these promising initiatives.

As Chairman of the Permanent Subcommittee on Investigations, I have pursued a bicameral and bipartisan investigation into supply chain security for almost 3 years. I have worked extensively with our Chairman, Chairman Collins, and am proud to have several of my findings and recommendations included in the Green-Lane Maritime Cargo Security Act, which I know will be the subject of a hearing next week, and I certainly applaud Chairman Collins' leadership on this issue.

Following our hearing last May and the two excellent GAO reports, I was pleased to see CBP and Commissioner Bonner acknowledge these findings and work to improve these programs. I am pleased to report today that CSI and C–TPAT have made substantive progress in the past 10 months, and are well on their way to becoming sustainable security programs.

With that said, considerable work lies ahead. These initial programs were only the first step in a constantly evolving process. We must urgently move to the next level of security—especially since trade is only forecast to continue its rapid expansion.

In preparation for this hearing, the Subcommittee wrote an extensive report that analyses the global supply chain. The Subcommittee staff's findings are troubling. In short, America's supply chain security remains vulnerable to the proverbial Trojan Horse—

[1] See Exhibit 9 which appears in the Appendix on page 373.

America's enemies could compromise the global supply chain by smuggling a weapon of mass destruction (WMD) or even terrorists, into this country.

Again, 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."

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 CSI, the Subcommittee found that only a *de minimis* 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.
- The Subcommittee found that an overwhelming proportion of participating companies in C–TPAT receive benefits prior to having their security profile validated. Only 27 percent of the participating companies have been subject 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.
- The targeting system employed by the U.S. Government to identify high-risk shipping containers entering U.S. ports is largely dependent on what some have phrased "the least reliable" form of data for targeting purposes, which includes cargo manifests and bills of lading. Moreover, the Subcommittee has found that this targeting system has never been tested or validated, and may not discern actual, realistic risks.

I will certainly speak to Deputy Secretary Jackson about that this morning.

The staff report makes several recommendations to enhance CSI, improve C–TPAT, and reform the automated targeting system.

But I would like to briefly focus on the initiative that I personally observed in Hong Kong, and that my two colleagues just talked about.

In December, I traveled to Hong Kong to examine the world's largest port. In addition to the impressive CSI team, and observing the close relationship between Hong Kong Customs and our CBP, I examined a promising screening concept piloted by the Hong Kong Container Terminal Operators Association. In Hong Kong, containers are screened with both x-ray and radiation detection equipment.

Effectively screening containers with both an x-ray and a radiation scan is the only definitive answer to the perplexing, and perhaps most important question that we are going to be examining today, "what is 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. Overall, CBP screens or examines only 5.4 percent of containers with what they call a non intrusive imaging (NII) machine, and less than 40 percent with radiation portal monitors (RPM). By any standard, any test, I believe that this is a failing percentage. We cannot afford to fail when it comes to public safety.

These numbers are low because to date, the Federal Government adopted a risk-based approach with the explicit goal of screening only high-risk containers.

Now, while this approach is fundamentally sound, the system used to target high-risk containers has yet to be validated or proven to accurately identify high-risk containers. Moreover, the validity of the intelligence used to enhance this system's targeting ability is increasingly in question.

So I think we need to both enhance our targeting capability and use technology to enhance our ability to increase inspections, again, without impeding the flow of commerce. I believe the Hong Kong concept holds great promise.

In Hong Kong, this system allows all incoming containers to be screened upon entry to the port without impeding the flow of commerce. In essence, the terminal operators, a private sector entity, have demonstrated that 100 percent screening can be a reality. The processes and policies to implement such a system are obviously quite significant. However, I believe the challenges that remain can be overcome, and I plan to work collaboratively with the Department of Homeland Security to solve these challenges.

It is also important to note that screening 100 percent of containers does not mean that 100 percent of images will be reviewed, or that our current risk-based approach is not the right one. This image is merely another piece of information, and more importantly, the system ensures that each container is screened for radiation, and that is important. In addition, if an event does occur, we would have the capability to go back and identify the container involved in the incident, and thus preserve our trade lines. We cannot afford to shut down all our ports and stop global trade, nor can we afford the likely outcome of a catastrophic event would have on our supply chain—U.S. Government mandated 100 percent screening.

Implementing this system will add another layer of security to the supply chain and demonstrate a true public-private partnership. We, the U.S. Government, should embrace this private sector initiative that increases our screening ability without impeding the flow of commerce. The task is too great for government alone. Industry and government need to work collaboratively, and move forward on programs and technologies to secure trade. Instead of security being a cost of doing business, it must become a way of doing business.

The bottom line is this: We are safer now, we are safer today than we were yesterday, but we have to ask the question continuously, are we safe enough? The question then becomes: How do we get there? In the words of the hockey legend, Wayne Gretzky, "A good hockey player plays where the puck is; a great hockey player plays where the puck is going to be." In other words, we cannot safeguard a post-September 11 America by simply using pre-September 11 methods. If we think that terrorists are not plotting their next move, then we are mistaken. We must find where the gaps are in our Nation's homeland security, and close them before an attack happens. This is the only way to guarantee our security.

To move in this direction, we need to implement 100 percent screening measures and we need DHS to validate that our automated targeting system effectively identifies high-risk containers. Currently, about 5 percent of all containers coming into the United States are actually inspected. By any test, this is a failing percentage, and we cannot afford to fail the public when it comes to security. We must secure our supply chain before we pay the high price of an attack. And this is what we hope to address today.

Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Mr. Chairman, thank you for all you are doing in an area of critical importance to the United States. You have focused this Subcommittee's attention on a critical national security problem, and the Nation will be more secure as a result of your initiative, and we are grateful for it.

Each year, as I mentioned a moment ago, about 11 million shipping containers enter U.S. seaports. Another 11 million containers enter the United States by truck, and 2 million by rail. Translating that to my home State, each week over 50,000 commercial trucks carrying containers cross from Canada into Michigan. Detroit is the number one entry point in the whole country for containers carried on trucks. Port Huron, Michigan is the number four entry point in the whole country. The vast majority of these containers are never inspected, and the challenge facing our country, as the Chairman has outlined, is what to do to address the national security threats that are posed by these containers.

The Subcommittee staff has conducted a bipartisan and bicameral investigation into U.S. Government programs designed to secure the global supply chain. The Subcommittee staff report makes recommendations with regard to key security risks facing our Nation, including the trash which is coming into the United States in containers that cannot be effectively examined.

The Subcommittee staff report confirms that a minimal number of containers are currently inspected, either domestically or overseas. The Subcommittee report found that Customs teams at three ports in France, Japan, and the U.K., refer a very low percentage of high-risk shipments for exams.

Another disturbing finding of the staff report is that the automated targeting system, ATS, the backbone of Customs security assessments, does not work with any assurance. Customs uses ATS to assign a risk score to each shipping container bound for the United States. The staff found that the ATS scoring system has

never been audited or validated to establish its effectiveness. Moreover, the data shows that ATS scores result in such a large number of containers being designated as high risk, that U.S. Customs officials stationed at the CSI ports often fail to request that each of the high-risk shipments be examined.

The C-TPAT program presents a different set of problems. C–TPAT confers a range of benefits on participants, many of which result in faster shipments for them. When C–TPAT first started, it conferred these benefits on all participating importers immediately upon receiving their application to join the program and prior to ensuring that the participant was meeting the program security standards. After the Subcommittee hearing in May 2005 questioned that approach, Customs changed its practice. Customs now reviews the security information of a C–TPAT applicant before allowing the applicant into the first tier of the program, which is an important change in the program.

The Subcommittee staff also notes, however, that the validation process being used by Customs examines only one supply chain for each program participant, even for companies that use multiple supply chains. To get a more realistic analysis of each participant's security practices, the Subcommittee report recommends that Customs examine more than one supply chain at more than one supply point.

As I mentioned, the Subcommittee report also addresses a key security issue which affects my home State of Michigan and a number of other States, which is the importation of containers carrying trash. Since 1998 Canada has shipped hundreds of thousands of trash containers across U.S. borders. According to the Department of Homeland Security's Inspector General's Office, in 2004 alone, Canada shipped approximately 100,000 containers of trash into Michigan. In addition, another 10,000 containers of trash crossed through nine other ports of entry on both the northern and the southern borders. During that period, Customs officials uncovered a number of instances in which Canadian trash containers carried more than just trash into the United States. The Inspector General has determined that from 2003 to 2004, Canadian trash containers brought into the United States illegal drugs, medical waste, and illegal currency.

Trash containers pose inherent difficulties in terms of supply chain security because it is difficult to trace the source and content of trash cargoes with any confidence. Even a trash importer with the best intentions is unable to monitor what is being transported in particular trash containers. The result is an unreadable x-ray scan, and I put a copy of that x-ray scan up on that chart over there, and you can see that it is unreadable because of the density of the cargo and its lack of uniform content. With other cargoes it is possible to know the content and to trace the origin, midpoint and ending point of the journey of the cargo, and then to 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, the Department of Homeland Security must take additional precautions before allowing trash containers to enter the United States, and until those precautions are taken and shown to be ef-

fective, we ought to end the importation of Canadian trash. They've got plenty of room to bury their own trash.

We should not be accepting any security risk to import Canadian trash. Current technology, as I indicated, cannot produce a usable x-ray image of a trash cargo because of the density and anomalous nature of that cargo. While other material such as concrete or bricks are equally as dense, they are uniform, and therefore, readily inspectable, and also, those products contribute positively to our economy. Their introduction into the flow of commerce provides building materials, helps create new jobs. Concrete and bricks pose lower security risks, since unlike trash, their supply chains can be monitored and made secure. In contrast, Customs would likely show that the security risk of trash and the cost associated with reducing that risk far outweigh any conceivable economic benefit.

A few years ago, Mr. Chairman, as you know—and you have been extremely helpful on this issue and we appreciate it—the security problems associated with trash containers crossing U.S. borders without effective screening technology, led me, along with Senator Stabenow and Congressman John Dingell, to ask the Department of Homeland Security's Inspector General's Office to review the effectiveness of the screening methods. The Inspector General's disturbing report, released in January of this year in an official-use-only version, identifies flaws and vulnerabilities with current methods to screen containers entering the United States.

The Subcommittee, in its report, has decided to release other official-use-only material today, and the report that I just referred to by the Inspector General should now also be made available, and I intend to do so.[1]

The Department of Homeland Security's Inspector General noted that improvements need to be made in the inspection process, and that the Commissioner should conduct a risk analysis and develop minimum requirements for selecting and inspecting trucks carrying trash.

Based on its investigation, the Subcommittee staff report makes the following recommendations, which I strongly endorse. Ban trash imports. Until it can be ensured that the supply chain of a trash importer is secure, we should not allow trash containers to enter the United States. The DHS should immediately adopt the Inspector General's recommendations to conduct a risk analysis, develop minimum requirements for selecting and inspecting trucks carrying Canadian trash if they are going to ever be allowed. Until these steps are taken and we have total confidence in the security of these containers, they should not be allowed. In the meantime, we ought to have an immediate moratorium on allowing trash containers into the United States.

I thank the Chairman for all he has done to direct the staff of the Subcommittee to look at all of the problems in this report, particularly for the one which I have just spent a few moments on, which represents an unusual and particular security risk to the United States, which is the import of Canadian trash. Again, thank you for your leadership, Mr. Chairman, and I have reduced, believe

[1] See Exhibit 16 which appears in the Appendix on page 491.

it or not, the length of this statement, and I would ask that the full statement be incorporated in the record.

Senator COLEMAN. Without objection.

[The prepared statement of Senator Levin follows:]

PREPARED STATEMENT OF SENATOR LEVIN

Each year, about 11 million shipping containers enter U.S. sea ports, another 11 million containers enter the United States by truck, and another 2 million by rail. Each week, 52,000 commercial trucks carrying containers cross from Canada into Michigan. Detroit is the number one entry point in the whole country for containers carried on trucks; Port Huron is the number four entry point. The vast majority of these containers are never physically inspected. The challenge facing our country is what to do to address the national security threats posed by these containers.

The Chairman is to be commended for focusing this Subcommittee's attention on this critical national security problem. The hearing held earlier this week concentrated on the specific problem of stopping the illegal transport of nuclear and radiological materials across U.S. borders. Today's hearing focuses on the two key programs which, in the words of the Customs and Border Protection of the Department of Homeland Security, are designed to "push out our borders" and inspect containers before they reach our shores. These programs are the Container Security Initiative (CSI) and the Customs Trade Partnership Against Terrorism (C-TPAT). Both programs were the subject of a Subcommittee hearing last year. Today's hearing and Subcommittee staff report continue that oversight effort.

The Subcommittee staff has conducted a bipartisan and bicameral investigation into U.S. government programs designed to secure the global supply chain. The Subcommittee's three year investigation has included document requests and letters from the Subcommittee, staff assessments of ten ports, and numerous meetings with both foreign and agency officials. The report released today identifies improvements needed in the key Customs programs, to address such problems as low inspection rates of high risk containers, the security of shippers' supply chains, and the effectiveness of the Automated Targeting System (ATS) used to identify high-risk containers. The Subcommittee staff report also makes recommendations with regard to a key security risk facing our nation: trash coming into the U.S. in containers that are not effectively examined.

The Subcommittee staff report confirms that a minimal number of containers are currently inpsected either domestically or overseas. At foreign CSI ports, 0.38% of containers were screened with either x-ray equipment or a physical exam, and only 2.8% of containers were screened with a radiation portal monitor. When U.S. and overseas data are combined, the data shows that Customs examines just 5.4% of containers either physically or with an x-ray, and uses a radiation portal monitor to screen less than 40% of incoming cargos. The Subcommittee report found that Customs teams at 3 ports (France, Japan, and the U.K) referred a disturbingly low percentage of high risk shipments for examinations.

Another disturbing finding of the staff report is that the Automated Targeting System (ATS), the backbone of Customs' security assessments, does not work as it should. Customs uses ATS to assign a risk score to each shipping container bound for the United States. The Subcommittee staff found that the ATS scoring system has never been audited or validated to establish its effectiveness. Moreover, the data shows that ATS scores result in such a large number of containers being designated as high risk, that U.S. Customs officials stationed at CSI ports often fail to request that each of the high-risk shipments be examined. If ATS designations are identifying too many containers for examination and U.S. Customs officials using the system are forced to apply their own criteria to select which cargos should actually be inspected at foreign ports, the current ATS is not functioning as intended. It needs to be either immediately refined or replaced since it is the backbone of the system.

The C-TPAT program presents a different set of problems. C-TPAT confers a range of benefits on participants, many of which result in faster shipments. When C-TPAT first started, it conferred these benefits on all participating importers immediately upon receiving their application to join the program, and prior to ensuring the participant was meeting the program's security standards. After the Subcommittee hearing in May questioned this approach, Customs changed its practice. Customs now reviews the security information of a C-TPAT applicant before allowing the applicant into the first "tier" of the program, which is an important improvement. The Subcommittee staff report also notes, however, that the validation process being used by Customs examines only one supply chain for each program participant, even for companies that use multiple supply chains. To get a more realistic

analysis of each participant's security practices, the Subcommittee report recommends that Customs examine more than one supply chain at more than one supply point.

The Subcommittee staff report also addresses a key security issue affecting my home state of Michigan, the importation of containers carrying trash. Since 1998, Canada has shipped hundreds of thousands of trash containers across U.S. borders. According to the Department of Homeland Security Inspector General's office, in 2004 alone, Canada shipped approximately 100,000 containers of trash into Michigan, an 8 percent increase over 2003. In addition, another 10,000 containers of trash crossed through 9 other ports of entry on both the Northern and Southern borders. During that period, U.S. Customs officials have uncovered a number of instances in which Canadian trash containers carried more than just trash into the United States. In fact, the DHS Inspector General has determined that, from 2003 to 2004, Canadian trash containers have brought into the United States illegal drugs, medical waste, and illegal currency.

Trash containers pose inherent difficulties in terms of supply chain security, because it is difficult to trace the source and content of trash cargos with any confidence. Even a trash importer with the best intentions is unable to monitor what is being transported in particular trash containers each day. With other cargoes, it is possible to know the content and to trace the origin, mid-course and ending point of the journey of the cargo, and then to 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.

In addition, current technology cannot produce useable x-ray images of a trash cargo, due to its density and lack of uniform content. This chart shows the x-ray image produced by a trash container at a Michigan border crossing. While other materials, such as concrete or bricks, are equally as dense, they are uniform and easily inspected. These products also contribute positively to the U.S. economy. Their introduction into the flow of commerce, for example, provides building materials and helps create new jobs. Concrete and bricks also pose lower security risks, since, unlike trash, their supply chains can be more easily monitored and made secure. In contrast, the security risk of trash cargos and the costs associated with reducing that risk far outweigh any conceivable economic benefit.

Two years ago, the security problems associated with trash containers crossing U.S. borders without effective screening technology led me, along with Senator Debbie Stabenow, and Congressman John Dingell, to ask the DHS Inspector General's office to review the effectiveness of Customs' screening methods. The Inspector General's disturbing report, released in January of this year in an "official use only" version, identifies flaws and vulnerabilities associated with current methods to screen containers entering the United States. The Subcommittee has decided to release other official use material today; this report should also be made available.

Based upon its investigation, the Subcommittee staff report makes the following recommendations, all of which I strongly endorse:

- Ban Trash Imports. Until U.S. Customs can ensure that the supply chain of a trash importer is secure and develops protocols ensuring adequate inspection of trash containers, Customs should not allow trash containers to enter the United States.
- Adopt Moratorium. Banning trash imports is the right answer to protect U.S. security. If a ban is not imposed, at a minimum, DHS should immediately adopt the DHS Inspector General's recommendation to conduct a risk analysis and develop minimum requirements for selecting and inspecting Canadian trash containers. Until those steps are taken, Customs should place a moratorium on allowing trash containers into the United States.
- Impose inspection Fees. If a trash import ban is not imposed, 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 security risks currently associated with trash containers.

I thank the Chairman for taking a close look at the problem of Canadian trash being imported into this country. As the DHS Inspector General has pointed out, it is a serious security risk for the country. I also commend the Chairman for his leadership in tackling the complex national security threats associated with container security in general.

Senator COLEMAN. Senator Levin, I want to thank you for your focus on this overall issue, but in particular, the laser-like focus you have put on this trash issue. I think that is what is needed if we are going to affect change. If we are going to make something happen, you need that. I want to pledge my continued cooperation and assistance because you are trying to do the right thing. So I want to thank you.

Senator LEVIN. Thank you, Mr. Chairman.

Senator COLEMAN. I would like to welcome the Hon. Michael P. Jackson, Deputy Secretary at the Department of Homeland Security. Mr. Jackson, I sincerely appreciate your being with the Subcommittee this morning, and look forward to hearing your testimony on DHS's efforts to bolster our supply chain security. As you are aware, pursuant to Rule 6, all witnesses before this Subcommittee are required to be sworn. I ask you to please stand now and raise your right hand.

Do you swear the testimony you are about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, to help you, God?

Mr. JACKSON. I do.

Senator COLEMAN. Thank you. I just want to say one thing, Mr. Jackson. I really do appreciate you being here. I know the full Committee will be having a hearing on the GreenLane bill that Chairman Collins has authored and you will be participating in that hearing. Our job is to do oversight, and I indicated early on—and I have been involved in this for a while now—we are safer today than we were on September 11, we are safer today than we were yesterday. But the reality is, the nature of this issue is such that we cannot rest on our laurels, and so our job is to keep looking at the soft underbelly. If you just look by way of example at what is happening in Iraq with IEDs, it is almost a cat and mouse game. We get a little better and they get a little better. I think it would be a great mistake for us to assume that somehow they are not getting better, that they are not seeing what we are doing, and so that is the challenge and the purpose of what we are doing here today.

I do want to thank you because you have been very helpful, and it is much appreciated by this Subcommittee.

TESTIMONY OF MICHAEL P. JACKSON,[1] DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Mr. JACKSON. Mr. Chairman, thank you for having me, and, Senator Levin, thank you for being here and for having me as well. I am very grateful for the work of this Subcommittee and very respectful of the work of this Subcommittee, and I am delighted to be here to help you understand that DHS is very much focused on the issues that you have been focused on.

Secretary Chertoff has repeatedly spoken about the importance of risk-based analysis. In our world we have to find the highest risks and apply prudential balance. As you said in your opening remarks, Mr. Chairman, that we have a balance between security and mobility. We can make a better balance. We can have better

[1] The prepared statement of Mr. Jackson appears in the Appendix on page 181.

security. We can make that equation iteratively stronger, and that is exactly what our commitment to do is.

I want to assure you that just as this Subcommittee has been focused on that matter, so to is the Department. I am going to tell you that I personally am committed to imposing a sense of urgency and supporting a sense of urgency about these matters, just as your Subcommittee work has done for us as well.

I will not try to go over a lot of facts and figures to reiterate what you have said, which is an important point. We have made transformational change in the security of the global supply chain in our Maritime World Security Program since September 11. We will spend this year at the Department of Homeland Security approximately $2.6 billion on maritime security efforts across the Department. If the President's fiscal year 2007 budget is enacted, we will have spent some $9.6 billion in this area in 4 years, fiscal year 2004 to 2007.

Earlier this week colleagues of mine from the Department, and from the Department of Energy, talked in more detail about some of the programs that you have already raised, and I shall not repeat the testimony there. I will try to supplement that.

What I will say is this really is an alignment. We need you and your strong report, Republicans and Democrats together with the Administration, to strengthen security on a continuous improvement basis. We also need our partners in the private sector to do just that too, and I am very grateful—you will hear from several of them today, and I am very grateful for the role that they have played, especially since September 11, in helping us do this transformational work in the marine world. So there is lots to do still, lots to do that we can do. In fact, we must be institutionally disciplined, just as you said, to keep this focus one step ahead of the bad guys. The area that we are focused in the maritime domain on most particularly, most urgently, is, of course, the weapons of mass destruction and preventing weapons of mass destruction from being intruded into the country from the maritime domain.

Our approach to security is a layered and evolving and continuously strengthening system. It is layered in ways that help us collectively through multiple mutually reinforcing tools diminish the risk that we associate with any specific failure at a specific point. So if you look at one layer, that is not the measure of how we can collectively bring security to the system. We got to take each of the weakest links in our layers and strengthen each of them iteratively, but we have to step back a little bit, and that is where I am going to try to talk today mostly, and say, where are the layers that need the most focus? What is it that we have that we can improve slightly to good advantage, and where do we have to dig deeper and really make more fundamental change?

It begs the obvious, but it is worth stating that this system we are talking about is a global system, and it is one that is driving our interdependent global economy. So what we have to do here requires the cooperation of multilateral government-to-government conversations. It requires the cooperation of domestic and foreign corporations. It requires the cooperation of technology partners to make the systems and tools that we will be talking about.

With whom should we partner and how? A fair question. But there is no question that we do have to make these partnerships with the private sector particularly in this global maritime domain.

Some of the first generation of layered security will give way to second generation tools. We will be able, in effect, to stand down certain type of tools and replace them with wholly new tools, and some of these tools will be iteratively strengthened in essentially the same groove, in essentially the same pattern, in essentially the same mode.

Let me just try to put into context where I would like to drive by trying to outline eight buckets of activity that we need to think about. Essentially, to outline our security there are four major moving parts or four components to our layered security: Vessel security, personal security, cargo security, and port facility security. So those four layer areas, we have programs in each. Then you have to divide it foreign and domestic. I think Rob Bonner was masterful at pushing the borders out early after September 11. I was at the time Deputy Secretary of the Transportation Department, and admired Rob's work, and having come to the Department of Homeland Security, I have enjoyed the benefit of the work that CBP has done in this area, and the Coast Guard has done in this area.

Most of the Federal programs in these eight buckets then can be clumped in some way or another. I would like to focus today on two particular areas that present significant opportunities for improving security. First, improvement regarding DHS's targeting of containers of highest risk, and second, related to this in this first bucket, tools to inspect containers, so improvement of the targeting, and improvement of the tools used to inspect.

And then a second area, I would like to talk for a bit just about deployment of the Transportation Worker Identification Card, the TWIC card. Both of these tools are areas I think of high opportunity for us.

Securing our borders requires us to dig deeper into what the Secretary is calling Secure Freight Initiative, which is an opportunity to look not only at better targeting, but enhanced inspection tools. CBP's automated targeting system is probably more effective than it gets credit for, and I am not so disappointed in that because all of the nuances of the system are not public matter. The components of it are a complex series of algorithms designed to help us select containers of high risk, and it includes data that is fed to us, essentially scraped electronically from the waybill, and also a large history file that allows us to pull up our inspections, our history of movements of individuals who are moving containers into the country. So these two parts of the ATS system are what makes it work.

Now, I want to say this is a first generation tool. Here is an area where we need a second generation tool, and if I could, I would just like to outline an idea that we are aggressively pursuing at DHS on what a Secure Freight Initiative might look like to help us dig deeper and plumb more sophisticated ways to get better targeting information, to enhance the ATS capabilities.

The supply chain is riddled with data about the pre-history of any inbound container movement that we do not collect. We have

no visibility into them we can't manage. It is resident not only in the ocean carriers, but in everyone who has touched a particular movement, the pre-history of that movement. In a short nutshell summary, what I think we need to do is mine that pre-history of every container movement to the maximum extent that is prudent and possible and that can be harmonized with the art of what works without imposing excessive burden, but we can do better. From the time an order is placed, the fulfillment of the order takes place and a container is sealed. It moves through the supply chain with intermodal movement, truckers, customs brokers, others having information about this. We can find a model I think to gather this, plus the waybill information that we currently have, and get a much richer pattern analysis for our targeting, our profiling of this container.

How would we do this in a global environment? I think what we have to do is look for a fundamentally different layer or business model on top of what we have. Let me try to describe it this way. If I can take on my left hand, and say, here are the governments, not just our government that needs this data, but I would argue that all governments that are involved in the international supply chain, moving containers across the globe. They need information about the security and a better knowledge of what is in them. On my right hand we have all the actors who touch this, essentially all private sector entities, some of whom are directly regulated by us, and others with whom I believe could be indirectly brought into an appropriate mix.

What I think we need is some intermediary institution, which I would like to see the industry work with the government to help create. I would be happy for DHS, and we will step forward and fund methods that would create such intermediary institutions, the hardware, the software, the institutional tools necessary to do this. But this data repository or data fusion center could gather information about movements in the global supply chain, and then could direct them to the government that needs that information. In effect, the data warehouse becomes a repository for information, and the government has a call upon that repository and drives that data in a real-time way into its own risk profiling analysis.

I have talked to multiple governments in the last 9 months about their interest in helping us try to find a more globally based and industry-centric partnered way to manage this data aggregation infusion. I believe there is strong interest in several of our strong partners involved in supply chain security to experiment in this area. I believe that industry can be helped to build this type of functionality. It cannot be done overnight. We cannot be too excessive or draconian in what we ask for. We have to work through issues about preservation of the privacy of confidential business information. We have to ask for what is reasonable. We have to look for what is possible, but what is reasonable and what is possible in the richness and density of this information will change and grow over time, and we need a new system, a more global system and a somewhat more powerful business model, I believe, to do that, just to do that.

So when your Subcommittee staff appropriately looked at ATS, the punch line was, we need better, stronger. I am in agreement

with that. CBP is in agreement with that. Secretary Chertoff is in agreement with that.

What we would like to suggest that this concept of secure freight can help create a much more powerful multiplier that takes the information, flows it into our ATS systems ultimately for the pattern analysis work that we would do, but can more powerfully and more quickly, honestly fuse this data.

Let me just say one thing about technology. There is nothing in what I have just described that is technologically impossible. The U.S. Government, however, is not the world's best technology integrator. What we need to do is find ways to work with the private sector to create a more nimble, more market-driven capability to do the initial aggregation. We would have to sit there with them side-by-side with government people, ideally with a multilateral team of auditors, inspectors and helpers. But we can, I think, with the proper incentives and support, financial and otherwise, create this capacity that just does not exist, and it will not take our lifetime to make this happen.

Let me switch to a second part of the secure freight idea, and it is this powerful idea that, Mr. Chairman, you have seen, and that your two colleagues spoke about eloquently this morning, of the pilot in Hong Kong. This week, Secretary Chertoff is in Hong Kong to look at this pilot himself, to kick the tires on it. But I would tell you, after extensive discussions with industry about the ICIS pilot and its underlying technology, and its underlying business concepts, that I find myself highly optimistic that this pilot can point the way to a collaborative network that can significantly enhance CBP's capability physically to inspect a large number of containers from points worldwide.

Again, I think this needs a little unpacking, so if I could take this one just one more layer. We should not either overly praise what is there, not ignore the fantastic opportunity that is in front of us. On the one hand this is a pilot. The data is not being used, as I understand it, operationally to manage security in the work stream that is existing right now. It offers tremendous promise to do exactly that, and after consultations on this topic, CBP has begun the comprehensive review of a large brace of this data to try to integrate this to our own targeting information, our own profiling information through the ATS system. So we will be able to say, here is a container of high risk. Let's look at these images. Let's see if this helps reconcile it or if it gives greater concern, and then we have to drive protocols that would allow us to inspect the things that need inspecting in a more physical and labor-intensive inspection.

But right now let's make no mistake, this is not an operational security tool. It is, however, I think, a transformation demonstration of the industry's commitment to put their own dollars to bear on improving security. They have agreed in Hong Kong to tax themselves for the purpose of improving security, and we should praise this and partner with these types of opportunities to take this type of system and make it an operationally more aggressive and solid tool.

I agree with what has been said. There are some export control issues why we might not want to put all of our technology abroad

in the world, but most sensitive parts of that have to do with the screening algorithms, the software. If we, in effect, globally network the images, as Senator Schumer was discussing earlier, we could keep the software, the analytical tools, protected appropriately, and do a much more substantial look at all of the high-profile containers with this type of additional tool. We could also randomly inspect more containers, and we could, obviously, and would want to, reconcile any alarm from a radiation monitor.

Right now the alarm is, in effect, turned off. It gathers data, but it shows no real-time alarm for us to reconcile. So we want to take what is very strong here, which I think is the industry's commitment to spend, their willingness to improve, their desire to partner with us, in fact, their—I am going to say—their aggressive creativity in putting together an opportunity like this. We have had some very substantial conversations with industry. I just report to you that after the Secretary gets back, we intend to try to bring this to a focus and see a path ahead. It is an area where we would want to come back to this Subcommittee over time, and work with you on exactly how we see that path unfolding.

I would just conclude with saying one quick thing about TWIC. If we talk about containers, and we talk about the port physical security, we talk about the vessels, we talk about the people, in the area of the personnel, we have to implement the Transportation Worker Identification Card program. It is too late, we have dithered too long. And I am here today to tell you that on Friday of this week, the Transportation Security Administration will publish a request for qualifications, seeking firms who are appropriately experienced and interested, to help us deploy certain components of the TWIC Program. This step tomorrow will be the first step towards operational deployment of the TWIC program as contemplated by Congress and contemplated by our Department. This deployment will include accelerated and parallel rulemaking work both by TSA and the Coast Guard, and it will include a procurement needed to help launch the operational program.

Secretary Chertoff has instructed his team to get this done as quickly as possible, and I can tell you personally that the pedal is pressing the metal.

Further details will be forthcoming as part of the rulemaking and procurement action, but this tool will add a valuable layer to our security needs.

I think I will stop there. I apologize for the length of my opening remarks, but I am grateful for the opportunity to have this dialogue with you.

Senator COLEMAN. Thanks, Secretary Jackson. I am actually uplifted to hear of the forward movement on the Transportation Worker ID Program. One of the great concerns I have is the current situation today where we do not know who is handling the product, and I think we are perhaps uneven in that situation, perhaps on the East Coast a little better than the West Coast, whatever it is, but this is an area in which we have to move forward. It is critically important. We can have the tightest global supply chain, and yet when the cargo is in our ports and we do not have clear control of who is there and who is picking it up and what they are doing with it, that entire system, it is only as strong as

the weakest link. And what you have identified is a weak link, and so I find it gratifying to hear that the pedal is to the metal on that one, and moving forward.

Let me just briefly talk, if I can, about the ICIS Hong Kong system. I want to make it clear, I do not think this is the cure-all, the silver bullet. I have no interest in ICIS. I am not sure if any parts are made in my State. I do not think so. It just seems to me that the challenge I have is when my constituents ask, is it technologically feasible, to have all cargo containers run through a radiation portal monitor. When my constituents ask that and I say, yes, and in fact, we do it in one place in the world, but we do not do it here, that is not a good answer.

So I look at this as being partners. You have done a very good job of really talking about the layers and this is not being used operationally. In fact, Senator Schumer said the system runs so quick as those containers go through as they are entering the Hong Kong Port, we are not checking each and every one of them. We have the image. We are seeing it going through a radiation portal monitor, which by the way, we do radiation portal monitoring of every car going through the San Ysidro land border crossing, about 50,000 cars a day in our land border crossings.

Mr. JACKSON. Yes.

Senator COLEMAN. So it appears to me that we know we can do it, so let's figure out how to do it quickly. That is my—you can see my colleagues, their reaction. So when you say highly optimistic, the way I understand it, I do not think any of us are saying this is the system and we need to implement this and it is going to solve all our problems. There are still a number of issues in the supply chain. But again, we have checked, in effect, 100 percent screening, and perhaps more important is that it is happening over there. That is another concern. If we screen it here and, God forbid, we even get it here and a device goes off here, it is still going to shut down our ports.

Mr. JACKSON. Yes.

Senator COLEMAN. On the other hand, we need to—and I think the genius of what CSI is about and C–TPAT is about is we have pushed our borders out. So I hope then, and what I am hearing, is certainly a willingness and a commitment to look at all of these options.

The fundamental underpinning of this is ATS, the system that we use to identify high risk shipments. Our report raises a number of issues, and you just touched upon some today. Clearly, we have to strengthen this system. A concern that what we have right now is we have bills of lading and manifest data—and I think it would be fair to say, even you said, that is not the best data. There is a lot of stuff that goes on before that we just do not know about.

I take it that it is technologically feasible today, from the time something is manufactured, let's say Target or Best Buy has a facility somewhere in China. They can put it in a container there, and I take it we have the technology today to determine whether that container is ever opened. Is that fair?

Mr. JACKSON. I don't think there is a production technology that has reliably demonstrated that container has not been penetrated. There are technologies that have been focused on the doors. There

have been technologies focused on the seals alone, but, frankly, you can pop the doors by the hinges, or you can drill a hole into a container. So what we are driving towards, where we have to be, is all six sides penetration monitoring and exception reporting, which could be real time. That is not Buck Rogers really, but it is not on the shelf today in a way that the industry would find, I think, something they would think is commercially viable.

Senator COLEMAN. I need to understand this because I do not want the good to be the enemy of the perfect right here.

Mr. JACKSON. Right.

Senator COLEMAN. The whole range of technology that allow us to say whether something has been entered. There is GPS to tell us where something is, whether it has moved outside. In fact, I just have to say that one of my frustrations on this Subcommittee when we were looking at Katrina is the government folks are saying things were lost in the supply chain. FedEx does not tell us that. So are we hesitant to move forward because we do not have a perfect system at this point in time?

Mr. JACKSON. No, I don't think it's that. I think our S&T Division is, at DHS, doing some extensive scientific and operational testing of these types of technology. The industry itself is doing that work as well. I think the component parts of the technology solution can be assembled, and then what you are talking about is a networked solution. It's a very intensive capital investment to create the networked solution. Without the network, you don't have the useful data in a time sensitive fashion, it is not as strong. So how you aggregate the technology, how you network the data feed, how you build it into an operational paradigm that makes a difference, these are all the component parts that have to be stitched together.

But I don't think it is unreasonable for you to press on this area, and we're pressing ourselves in this area.

Senator COLEMAN. One of the concerns we have about the targeting system is some would say that it hasn't been fully tested. We haven't done a red team test and tried to find a hole in the system, which is what we did with the GAO report, and smuggled two dirty bombs into the country. Can you give me a sense of your confidence in ATS today, and whether in fact we are in the process of doing the kind of testing that would at least raise the confidence level of some of us on this side of the bench?

Mr. JACKSON. It's our job to help you raise your confidence level, and we want to give you the information to do so, and we want to make a system that will make you feel like it is something that is as good as it can be.

I believe it is a strong and powerful tool. I do not believe it is a perfect tool. It is transformationally better than what we had on September 11, and I believe to take it to the next step, you can work in two grooves. You can work to do the type of peer review, peer analysis that you have called for, and which our Inspector General has suggested. We are doing that. We have a firm—I think your staff has been briefed—that is under way with just such an effort today.

The idea of red teaming, that is an inherently solid thing that ought to be part of our ConOPS for all of our modes in transpor-

tation security. So we are doing more there. We can take that tool and make it stronger.

What I was saying earlier about secure freight is that there are inherent limitations if we limit ourselves to the data that comes in by virtue of just a waybill. When you make that move from gathering just this data, which is readily available and electronically submitted, to fusing data from multiple other vendors, you have to take a different step, and I think, take on a different business model. Again, I do not think that this is something that is out of the realm of possibility in the near term to make real. I want to be able to say when I have left my job in 3 years, that we left this system behind, it is working, it is humming, it has made a big difference.

So that's the sort of timeframe, in my mind, that I think we should be thinking. It's not decades to do this. It won't be months, but it's not forever.

Senator COLEMAN. Let me just follow up with this question about my firm belief that we have to do the inspection before it reaches our shore. I have a chart here that we used the other day. This chart shows out of all the targeted containers [1]—we identify through ATS-containers that are high risk, we then make requests to have them examined, and then we get a percentage of those requests complied with, higher in some areas such as Hong Kong, less as in other areas like LeHavre, France. What can we be doing to make sure that when we request a container be inspected, that the host government, the host country, do the inspection?

Mr. JACKSON. I think we just have to be very firm. What I was told about this particular set of data is that we have made progress on the two bars that are lower on that chart since that data point was taken. But, again, this is something we just have to work on a case-by-case basis with each government. We have to show them that this is a compelling priority for us, and it's not going to be easy in every circumstance, but I think we have to be determined, and we can.

We will use multiple ways to help make that work. The Megaports Initiative puts technology overseas to help in some of these cases. Our own people there, deployed in the right way, can make a big difference. It is a partnership, and like all young partnerships, this one is still evolving, but I think growing stronger, and to me, is an impressive foundation.

Senator COLEMAN. Thank you, Mr. Secretary. Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman. Thank you, Secretary.

Mr. JACKSON. Yes, sir.

Senator LEVIN. I want to just pick up where the Chairman left off in terms of the requests that are made to foreign governments. You say we have to show them a compelling reason for them to carry out the kind of inspections or the need for that. Why is that not automatic? Why do we have to ask them anything? We just tell them we are not going to accept the container.

Mr. JACKSON. We can do that, and that is the ultimate lever, and I believe we should be absolutely willing to drop that lever.

---

[1] See Exhibit 7 which appears in the Appendix on page 371.

Senator LEVIN. Is there a reluctance to just say, "Unless you folks carry out these kinds of inspections, that we are just not going to allow it in?"

Mr. JACKSON. No, I don't think there is a reluctance. There is not an institutional instruction order or demand that that not happen. In fact, I would say there is some strong leadership incentive to say, "We've got a 24-hour rule. It's working. Don't load." So I believe we can do more of that.

Senator LEVIN. I am not satisfied with that answer. It seems to me it ought to be an automatic, just simply say—let me go to Tokyo, let me just give you the numbers in Tokyo. I do not know if that is on the Chairman's chart or not, but in any event, let me use these numbers. It is kind of hard to follow them without them being on a chart, but here goes. Our automatic targeting system identified 5,600 high-risk containers at the Port of Tokyo. This is from February 2005 to February 2006, 477 exams were requested by the CSI personnel, and then 430 exams were conducted by Tokyo officials, so about 10 percent of them, roughly, were not examined.

Now, first of all, I am not sure I followed your answer as to why it is after we identify 5,600 high-risk containers, there is only about 9 percent that lead to a request for an exam. I did not quite follow your answer on that one. Maybe I ought to ask you that one first and then lead up to the fact that the Tokyo officials did not carry out the exams on 10 percent after we requested them to do so.

Mr. JACKSON. Let me start with one point that I think is most important, which is all of the containers that are identified as high-priority containers will be——

Senator LEVIN. Is that the same as high risk?

Mr. JACKSON. High risk, yes, sir, sorry. High risk—you actually have the nomenclature right, I didn't—will be inspected either abroad or in the home port at home when it arrives.

I agree, and we all agree, that it is better to push as much of that out as far as possible. I'm going to have to just tell you that we actually do that screening inspection for all of the ones that are the high-priority containers.

Your question, it is a good question, is a fair question, it is an operationally important question, is how do we get it pushed out farther?

Senator LEVIN. No, that is not my question, but let's go back to what you said. How do you know that all of those containers are in fact inspected when they get here?

Mr. JACKSON. They track each of these, and they reconcile them through CBP, and they keep records of—there's a score on the algorithm, and when that score is triggered, those containers are targeted for inspection and must be inspected. We inspect 100 percent of all those high-risk containers.

Senator LEVIN. So those 5,600 high-risk containers identified at the Port of Tokyo, are all inspected, either there or here?

Mr. JACKSON. Yes, sir.

Senator LEVIN. And you've got data which you could show us to confirm?

Mr. JACKSON. I'm assuming we could show you the CBP audit trail on these issues.

Senator LEVIN. Would you do that, so we can follow how——

Mr. JACKSON. I would be happy to walk through that.

Senator LEVIN. OK. I do not know why they are not all examined overseas. What is the reason for that?

Mr. JACKSON. Senator, I am going to have to plead that I would like to get back with you with a more complete answer. Let me give you a very partial answer. Part of this is a limit on the resources that we are asking another government to bring to bear to do our work. If we know we have this safety net, which is we are going to inspect 100 percent of all these containers, we do engage in, I believe, operationally a triage process, which is, in effect, to say if we are absolutely, positively worried about one that we think must be inspected, we ground it. If we can get them to inspect it and clear it, we clear it and allow it to come forward.

I am confident that on a port-by-port basis there are circumstances about the scheduling of staff, the equipment that's available for screening, radiological screening and VACAS type of screening, that impose limits on this. I would hypothesize that there are, I'm going to say, institutional barriers in some cases that we need to work. So all of those levers, this is why your support for ICIS is important too. If we have the technology there, and we can run things through and look, then we are in much better shape.

Senator LEVIN. All right. Who do you think should bear the burden, the cost of that inspection? Should it be the buyer or the seller basically?

Mr. JACKSON. Yes.

Senator LEVIN. What is the deal, 50–50? Just real quickly. I am going to run out of time.

Mr. JACKSON. The shipper ends up paying the cost of moving goods throughout the system, and how we allocate it, we are going to end up having to talk through that equation.

Senator LEVIN. That the shipper should, the shipper being the seller—the seller and his shipper should pay that cost?

Mr. JACKSON. Whoever is receiving these goods, who is paying for the container to be moved is going to pay the ocean carrier, the dredge move, the manufacturer that closed the box and ships it over to you.

Senator LEVIN. We will have to leave that one, because I think it is an important question, but we are not going to resolve that here. Now, 10 percent of the 477 exams that were requested by our people were not conducted by Tokyo officials. My question is, why should it not be automatic? We make that request. It has got to be done or else it cannot be shipped. Why not just tell them that?

Mr. JACKSON. Can I unpack that example, and get you back a detailed answer about what happened there?

Senator LEVIN. Well, you can, but let me just say, well, that is true with almost all the ports, so it is not just what happened there. I am not picking on Tokyo. This is true with all the ports. And I think our Chairman pointed out, and this chart points this out, that I think our Subcommittee staff found that 18 percent overall of the requested exams are not carried out. That is high-

risk containers where it is a very small percentage that we are asking——

Mr. JACKSON. They are not carried out overseas, but they are conducted when the container arrives.

Senator LEVIN. I know, but these are ones where we specifically ask the officials in that overseas port to do it, and in 18 percent of the cases they do not. This is a part of a part of a part. These are the highest risk of the highest risk.

Mr. JACKSON. I would like to get some better data for you, sir.

Senator LEVIN. OK. My question is, why don't we just make that automatically a precondition of shipment. Folks, if you do not do it there, we are not going to accept it in our ports. That is the question, OK?

Mr. JACKSON. We would probably have to then manage the protocols that would define what we would ask for with a greater degree of granularity than we do today if we are going to make exit/entry around the ask.

Senator LEVIN. We have a declaration of principles with every single country where a CSI port is established. Why not make that one of the declarations of principles?

Mr. JACKSON. I would have to look at the declaration. I haven't read that, sir.

Senator LEVIN. OK. Just yesterday the GAO provided the Subcommittee with preliminary results of a report that they are working on with regard to ATS, where the GAO also confirms what the Subcommittee staff report says, that ATS is ineffective. Are you familiar with the GAO report to this Subcommittee?

Mr. JACKSON. I have not read it, sir.

Senator LEVIN. I want to save a minute for the trash issue, but I want to just give you an article from the *Detroit Free Press* of March 29, which shows that the inspectors are waving through long lines of trucks without inspection in order to speed up the process, and that they are doing this on the instigation of their supervisors.[1] I will not ask you to comment today unless you are familiar with it. If you are——

Mr. JACKSON. I'm not, but I would be happy to look into it.

Senator LEVIN. If you would do that for the record.[2]

Now, I will take my last minute on the trash issue. Current technology, and maybe no technology, can produce useful and usable images of trash cargo. It is too dense, it is too anomalous. You have seen the x-ray image, which I put up there before, which was taken at a Michigan border crossing.[3] You just cannot see the contents of the container because x-rays cannot penetrate the contents because of its density.

At Tuesday's hearing, our Chairman, Senator Coleman, showed the same picture to Mr. Oxford, who is head of the DHS's domestic nuclear detection office, and asked him whether he could tell whether there was a dirty bomb in the trash truck. Mr. Oxford stated the current picture showed very little content and that they are working on the next generation of x-ray machines.

---

[1] See Exhibit 14 which appears in the Appendix on page 436.
[2] See Exhibit 19 which appears in the Appendix on page 465.
[3] See Exhibit 15 which appears in the Appendix on page 440.

If your head of the DNDO says that x-rays cannot adequately show what is in a container—which is obvious to us, just look at the picture—why not just simply tell the Canadians, "Folks, there is a security issue here for us. We cannot determine with any credibility or confidence what is in these trash trucks without unloading every trash truck and inspecting it. You are going to have to end these shipments until there is such technology, and by the way, you guys have more land in Ontario than we do in Michigan." This is not the only State affected. There are, I think, three other States, including New York, where trash is shipped from Canada or Mexico into our country.

That is my question of DHS, why not just simply say, "We cannot effectively inspect. Until that is doable, you are going to have to bury your own trash."

Mr. JACKSON. Sir, we have not reached the conclusion that that measure is a requirement. We have, however, taken this issue, which you've been a very eloquent advocate for, for which I am personally grateful, and we have launched a process that will be very shortly completed, the first step of which is due by May 1, which is an analysis of the technical and operational means that we have. You are right about this image. We can do radiation detection work. We can do physical inspections. We do that. We follow these trucks to the dump on a random basis, and literally crawl through the slime with them to do this work. We have multiple different layers of operational controls here. We have no perfect technology——

Senator LEVIN. It is not a perfect one. There is not one which is anywhere near perfect. I mean the pictures are useless. You are not going to inspect every truck at the dump. If you follow one out of 500 you are doing well probably. The radiation cover is just one of the many problems. So the bottom line is what I said, there is no effective way of inspecting. There is a security issue in this. Would you agree with that?

Mr. JACKSON. There is a security vulnerability.

Senator LEVIN. In May you are going to let us know whether or not we should tell the folks——

Mr. JACKSON. In May we are going to come back and we are going to unpack that security vulnerability with more detail, and tell you the types of options that we think can be put in place against the problem, and I am happy to make sure that we come up and brief you as soon as the first work is done. That will be followed by a requirements document and production of exactly how you would manage this process, pay for it, and operationally deploy the tools needed to do that, and we will keep you in that process all the way.

Senator LEVIN. Two questions. Make sure it happens promptly, and, number two, make sure one of the options there is just stop it until we have an effective technology. I want you to include that option. Will that be included?

Mr. JACKSON. I'll promise to make sure that the option is added to the list of options.

Senator LEVIN. Mr. Chairman, thank you for your support and your patience.

Senator COLEMAN. Thank you, Senator Levin.

I am actually going to do a quick 5-minute follow up because I want to pursue what I ended with and you focused on, and that is the discrepancy between those containers that are identified as high risk, those where requests were made and those actually examined. You have a significant number that are identified as high risk for a range of reasons, could be drug smuggling or whatever. Then we make the request, which is a lesser number, and then after we make the request, ultimately, some are examined. I concur with Senator Levin, if we make a request, if we believe something is problematic, we should just say it is not coming here unless we take a look at it.

I appreciate your telling the Ranking Member that you would show us the audit trail. I have to say, Mr. Secretary, that neither this Subcommittee staff nor the GAO has to date seen any audit trail. In my Chairman's letter, I specifically requested that, and we have yet to see anything that demonstrates there is an audit trail. So we have heard the testimony from you and others saying, yes, we identify things as high risk and we inspect them here.

I appreciate your recognition that it really should be inspected somewhere else before it comes into our ports, because, God forbid, we miss something and something happens at the time we open the box, our commerce will be shut down. But beyond that, we really do request to see that audit trail. If there is not one, then we have to recognize that and deal with it. But I can tell you that as we sit here today, neither this staff nor the GAO has seen any evidence of an audit trail, and we find that particularly disturbing.

One other question with C–TPAT, because one of the things we do—and we touched on it briefly—is this public-private partnership. We agree that we need to work with foreign companies that run ports around the world and in this country if we are going to be secure. That is the reality; is that correct?

Mr. JACKSON. Correct.

Senator COLEMAN. We need to work with private companies. And in fact, Senator Levin, in the whole ICIS, the program in Hong Kong, includes no Homeland Security grants. In fact, the private sector said, we are going to do this because we are concerned about what happens if something goes wrong. But one of the concerns even with the C–TPAT program, which is this partnership with the private sector where folks get points, is that C–TPAT members receive free passes from some screenings if we think it is secure enough. On the other hand, we have a significant number of companies that we have not been validated to determine their system is secure. Can you tell me how many companies involved in the C–TPAT that we have actually verified?

Mr. JACKSON. We have 5,800 companies enrolled in C–TPAT right now, and 27 percent of those companies have had a completed validation.

Senator COLEMAN. Have you thought about using a third party, bringing someone else in just to pick up the numbers?

Mr. JACKSON. Yes, sir, I have. It is an option that I have asked CBP to come back and give us details on. I am personally quite open to the third-party intermediaries. The government has to own the security function. The government has to be able to manage that, but I am not closed at all to the idea that there might be mul-

tiple ways to accelerate our validation process here, and strengthen it.

Senator COLEMAN. And, again, we are talking about a partnership. We do not have to do it all by ourselves, and if we simply cannot do it, then I would hope we would reach out and work with some others so we can bring that number up.

Can you tell us today the percentage of cargo containers that are at least screened for radiological material, those that go through a radiation portal monitor? Do you have numbers on that?

Mr. JACKSON. I do. This is in the U.S. ports, we screen with RPMs, radiation portal monitors, before they leave the port. Right now it's 67 percent of the exiting containers being screened, and we have a deployment plan that will bring that to 98 percent by December 2007.

Senator COLEMAN. The follow-up question, again, with the belief that it is best to screen before they get here, what is your vision—do you have a vision that says 100 percent screening at some point in time before they get to U.S. ports?

Mr. JACKSON. I think it is difficult always to throw the 100 percent screening, because just as this 98 percent screening, the marginal investment to get that last 100 percent guarantee is probably not worth that same lay-down. We could use, for example, on that last 2 percent, a very high proportion of random inspections using hand-helds, and I think, therefore, crunch that 98 number up higher, but maybe not to 100.

Similarly, on the problem abroad, first, why I am so committed to explore the ICIS business model is, from the major load-out ports that are moving cargo our way, this is an opportunity to accelerate and strengthen in a meaningful way our capacity to screen abroad. But there are many smaller ports where this degree of scrutiny may not be cost effective, or where we may simply not be able to get the government or the terminal operators to play along with that. So can we get a lot done? I believe that there is a real prospect of doing just that. I am hesitant to make a firm commitment, say, yes, let's drop the hammer and say 100 percent everywhere by this date.

Senator COLEMAN. In the end I understand that.

Mr. JACKSON. The overseas part.

Senator COLEMAN. I think the best vision, that is, push out the borders and then do things like Megaports, and work with companies like Hutchison in the Bahamas. I know some of my colleagues, and I had concerns about the CFIUS process. I believe we need to do 45-day reviews, and I thought the law was broken when we did not do a 45-day review for the DP World situation. On the other hand, I am seeing reaction here that you see the word "foreign" and all of a sudden that is bad. What would be bad is if we do not work with other entities, we do not work with corporations, we do not work with other countries, and we try to do it all ourselves.

Mr. JACKSON. Right.

Senator COLEMAN. Then we will fail.

Mr. JACKSON. That is exactly right, sir.

Senator COLEMAN. What I would hope though is that we would have this focus on pushing it out and see, if not 100 percent, let us significantly improve the numbers that we have now that Sen-

ator Levin and I am concerned about. The ICIS prototype shows us it can be done.

Mr. JACKSON. I want to just leave one other thing on the table with you that I think is a cause for considerable enthusiasm and optimism on the radiation screening. You heard from Vayl Oxford earlier this week to talk about our next generation of advance spectroscopic portals, so called ASP systems. This is an area we are spending half a billion dollars this year at DNDO. I am very pleased at the quick start-up, and, frankly, grateful for the comments from your Subcommittee on some of their initial work.

I think we can move to a much more effective tool in this area, and we can layer on top of that some pattern recognition software that would allow us to be more effective in looking at the image before us. We can look at tools like throwing up false images for our inspectors so that they can be tested, probed and pushed, and we can grade them and watch them and monitor their capabilities for doing this. Technology here offers some very near-term windows for major improvements. So as we think about how to take an ICIS type business model, we have this overlay of an intense investment that the Congress and the Administration have committed to this area, where we will get a much more meaningful tool. Sometimes we will be able, just on the basis of knowing the source, to be able to shoot that one through and say, yes, that is what should be coming from the background radiation associated with what we have in the waybill and other information about that load.

Senator COLEMAN. I appreciate that. My concern is that I hope we take advantage of that.

Mr. JACKSON. Yes, sir.

Senator COLEMAN. I mentioned the Katrina hearing. It was extraordinarily frustrating for me to sit up here and listen to government officials talk about things being somewhere in the pipeline, when the 21st Century technology of not just FedEx, but small companies, can tell you exactly in the pipeline where that carburetor is, where that pair of shoes that you bought, and this is one area which government cannot afford to be operating in the 20th Century when industry is operating in the 21st Century. So I applaud the vision, and I just hope that you can push the bureaucracy really hard, so that we are not stuck with 20th Century technology when we have 21st Century security needs.

Mr. JACKSON. Yes. It's an urgent priority and it is a constant push to try to prioritize men and women who are doing 1,000 important things, to do 1,001, but this one is something that is very much on the Secretary's radar screen, it's very much on the Coast Guard's, the CBP's, the DNDO's. Our team is focused on this.

Senator COLEMAN. And we appreciate that and appreciate your appearance here.

Mr. JACKSON. Thank you.

Senator COLEMAN. Thank you, Mr. Secretary.

I would now like to welcome our final panel of witnesses to the hearing: Christopher Koch, President and CEO of the World Shipping Council here in Washington, DC; Gary D. Gilbert, the Senior Vice President of Hutchison Port Holdings of Oakton, Virginia; and, finally, John P. Clancey, the Chairman of Maersk Incorporated of Charlotte, North Carolina.

Clearly, the purpose of this hearing is to examine the current status of global supply chain security and analyze ways we can improve that security. An integral partner in securing the supply chain security is the private sector, and I was pleased that the Secretary made specific mention of that today. You are the companies that manufacture the goods, import the products, ship the containers, and operate the ports. And without your invaluable assistance, our government efforts would be far less successful. So I appreciate your attendance at today's hearing, and I look forward to your perspective on supply chain security.

Before we begin, pursuant to Rule VI, all witnesses before this Subcommittee are required to be sworn. I would ask you to please stand and raise your right hand. Do you swear the testimony you are about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. KOCH. I do.

Mr. GILBERT. I do.

Mr. CLANCEY. I do.

Senator COLEMAN. Thank you, gentlemen.

We have a timing system here. When the light turns from green to yellow, if you can sum up. Your written statements will be entered into the record in their entirety. We are just going to go from my left to right, and we will start with you, Mr. Koch, first, followed by Mr. Gilbert, finish up with Mr. Clancey, and then we will have some questions.

Mr. Koch, you may proceed.

TESTIMONY OF CHRISTOPHER L. KOCH,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, WORLD SHIPPING COUNCIL

Mr. KOCH. Thank you, Mr. Chairman. Thanks for the opportunity to be here today. My testimony is somewhat lengthy, and I will just summarize it in the following manner.

The overall strategy and objectives that the Department of Homeland Security is using to try to address this challenge is something that we believe is fundamentally sound. It is the implementation that can be consistently enhanced and refined, and we appreciate the Subcommittee's review of how that can be done most effectively.

For maritime security strategy to be looked at, there is a vessel piece, there is a people piece, there is a port piece, and there is a cargo piece. And, obviously, today's hearing is focusing really on the cargo piece.

Your questions to the witnesses, or at least to me today, also asked for comment on our views on foreign investment, and I would like to start with that. Ninety-seven percent of the containerized cargo coming in and out of the United States is carried by companies that are foreign owned or controlled. The vast majority of the cargo handled through U.S. ports is handled by marine terminal operators that are, in fact, foreign owned. This is an industry, even though it is a critical national infrastructure, that is clearly basically run by foreign-owned companies.

[1] The prepared statement of Mr. Koch appears in the Appendix on page 187.

These companies, represented by people like Mr. Clancey and Mr. Gilbert, are working very hard to be partners with the U.S. Government, to come up with good solutions in this regard. And so to answer the Subcommittee's question, my view on foreign investment is that it is an essential part of the smooth functioning of the American economy. We would hope that the American Government would reach out and work to develop partnerships with these actors, particularly as you look to things like ICIS, as I will get to later. If we are really going to embrace that concept, we have to understand that the people operating those post terminals where that equipment is going to be are going to be foreign terminal-operating companies, including companies like Dubai Ports. So we really have a strategic question to ask ourselves: Are we comfortable with this or not?

My hope is that this Subcommittee and the Congress would say that they are comfortable under the right terms, making sure that can be done.

Let me turn now to the cargo issue. The strategy of the government is something we fully support and think is very important, and that is to do the cargo risk assessment before vessel loading, and if there's any cargo that is deemed high risk, it should be addressed before it is put on the ship and brought to the United States. That is the proper security strategy for the government to embrace. The strategy has various pieces in it that buttress this. As you have pointed out, Mr. Chairman, there is the screening for risk, there is CSI, and there is C–TPAT. But the overall objective is to inspect any container we have a question about. We use container inspection technology that includes both the NII type equipment, which produces the kind of image that Senator Levin was pointing to earlier, and also radiation scanning equipment. The present objective is to use NII or full devanning inspection of any container there is a security question about, and radiation scanning of all containers.

Now, ICIS is a very attractive concept, but it is not yet an operating system. It presently doesn't analyze or check the data generated about the boxes itself. What is encouraging about it is that the pilot appears to be demonstrating that the quality of the information that is generated by this technology is something that can have great use. But there needs to be an understanding about the assumptions of how this would actually work.

If the assumption is that this technology is going to, in fact, be used to actually inspect every single container, you have to put it in context to understand the difficulty with that. Presently, we understand it takes 4 to 6 minutes for a trained CBP expert to look at one of these images and come up with an analysis of it. If you apply that to a container ship holding 4,000 containers, that is about 14 days' worth of work for a single individual.

We understand the concept as being one that can expand the tools available to the government to inspect any container before vessel loading at a foreign port where you have a question about a box—not that every box is going to have to go through the inspection process. But it's these kinds of questions that need to be thought through as this concept is considered and it is rolled out. As I said, it is a tool, but to make it part of an operating system,

Customs and DHS have to sit down and figure out how they're going to use this tool, how the data's going to be transmitted, how the protocols are going to be established, and how to develop the cooperation and receive the permission of foreign governments.

There will be nuisance alarms that get set off repeatedly with this techology. How are those going to be resolved? By whom? All are very important questions, and we would urge that the concept not be rolled out with the assumption that we will consider those things after the containers have been loaded on the ship and it's sailing for the United States, because that's the wrong time to figure those things out.

You've also asked the question about what we think the priorities are going forward to enhance maritime security. I would start with basically four.

The first is, which has already been touched on today, the World Shipping Counsel believes that we should improve the data used for risk assessment by CBP's Automated Targeting Center. The carrier's bill of lading and the current 24-hour rule were a very good start. They do clearly have good value, but they are not adequate by themselves, and we should improve that.

Second, the TWIC card should be rolled out. It was very good news to hear Mr. Jackson today stating that there will be a Federal Register notice tomorrow that's going to start that process. It's probably the most important thing that can be done to improve U.S. port security in the immediate future.

Third, we fully support a priority examination and analysis of the ICIS project and the technology and how it can be integrated into the basket of tools that the government has to improve maritime security.

And, fourth, to continue to do what Customs is doing to enhance C–TPAT, enhance CSI, and build closer, more cooperative relationships with foreign governments and the rest of the trading partners working in these supply chains.

The U.S. Government cannot do this by itself. It needs the assistance of foreign governments, and it needs the assistance of the rest of the people working in the supply chain, and those relationships are understood by the Coast Guard, who's working with the foreign governments, and carriers and terminal operators. And it's understood by Customs, and that needs to be nourished, as they are doing.

And, finally, we would simply again repeat our hope that, in looking at these issues and in passing legislation, that the Congress resists the temptation to in any way restrict foreign investment or to otherwise impair the growing, constructive relationship that is in place right now between members of the industry and the U.S. Government to solve what is clearly a very difficult challenge for all of us.

We are transporting this year probably between 11 and 12 million containers into the United States. That's an enormous challenge just from a commerce perspective to handle this volume efficiently. You have been to L.A.-Long Beach. You've seen the volume going through there. Without the continued investment and commitment of these present companies in this business, the U.S. economy will have a very serious difficulty just handling cargo.

So what has happened over the last several weeks has been perhaps turned into a good wake-up call. How can we do something constructive to improve maritime security? And we are certainly prepared to work with this Subcommittee and you, Mr. Chairman, in any way possible to see that is what results from all of this.

Senator COLEMAN. Thank you, Mr. Koch. Mr. Gilbert.

TESTIMONY OF GARY D. GILBERT,[1] SENIOR VICE PRESIDENT, HUTCHISON PORT HOLDINGS, OAKTON, VIRGINIA

Mr. GILBERT. Chairman Coleman, Senator Levin, we are very honored to be here to give our perspectives on the vital issue confronting the risk of nuclear smuggling and supply chain security.

Chairman Coleman and Senator Levin, we are very pleased to be here to talk about nuclear smuggling and supply chain security. I want to thank you personally for coming out, for your leadership, as well as your staff. Three of them are here—Ms. Kathy Kraninger, Brian White, and Ray Shepherd—on the many trips they've made to see firsthand what is happening in supply chain security.

HPH has been in the maritime business for 139 years originating the first registered company in Hong Kong in 1866, the Whampoa Dock Company. HPH is the global leader in the container terminal operations handling 51.8 million containers in 2005. We are located in 42 locations in 20 countries, and approximately 40 percent of the containers coming into the United States were either loaded or transshipped through an HPH facility.

To date, HPH operates no ports within the United States. Given that fact, you might wonder why our company would be interested in partnering with the U.S. Government on a maritime security agenda.

First, we share the shock and outrage that all Americans felt on September 11 and realized the world had changed on that fateful day.

Second, as the world's largest marine terminal operator, we know that we may be just a single terrorist incident away from having our whole global system fail.

To a large extent, the modern global logistics system is a result of the revolution in transportation that has gone unobserved by most Americans. I have witnessed firsthand the fruits of hundreds of billions of dollars of investment to construct an intermodal transportation system that is efficient, reliable, and low cost for its users. As chairman of the Corporate Security Committee of HPH, I also know that the system is vulnerable to being exploited or targeted by terrorists. Should an attack lead the United States to close the ports even for a short period of time, the consequences to my industry and those who rely upon it would be devastating.

The potential for the cargo container to be exploited for an act of terror has been borne out 2 years ago in Israel in a sparsely reported event that took place 3 days after the train bombings in Madrid. On March 14, 2004, two Palestinian suicide bombers were intercepted before they reached their intended targets of several fuel and chemical storage tanks in the port of Ashdod. The Pales-

[1] The prepared statement of Mr. Gilbert appears in the Appendix on page 205.

tinian militants killed themselves along with 10 Israelis, and wounding 18 others. They reportedly evaded the security at the port facility's gate by being smuggled from Gaza in a container outfitted with a secret compartment and an arms cache—the first majority where terrorists both exploited a container to get to their target and that their target of choice was a port facility.

Our industry is so vulnerable to disruption. The terminal you visited, Hong Kong International Terminal, has a combined input of about 7.5 million containers. To support that kind of throughput, the facility operates 24 hours a day, 7 days a week, 365 days a year. Each day, upwards of 10,000 trucks drive through the gates of that terminal. A 96-hour closure—and we have them from time to time for typhoons—strands tens of thousands of containers, backing them up for upwards of 100 miles back into China.

But our Hong Kong terminal as well as our other 41 terminals around the world can be seriously affected by closures elsewhere in the system. Our system got a flavor of that in October 2002 when a labor dispute on the West Coast of the United States led to a 10-day closure of the ports. According to Robert Parry, president of the Federal Reserve Bank of San Francisco, the estimated cost to the U.S. economy was $1 billion a day for the first 5 days and rising to $2 billion each day after. Major retailers like Target Stores from your State became deeply concerned that their merchandise might not reach their shelves for the holiday season. Over 100 major container ships were stranded at the port outside of Los Angeles, causing major disrupts and delays. I suspect this should be a real wake-up for us in looking back at history.

We expect that a breach may be involved in a dirty bomb, which will lead the United States and other States to raise their port security alert to its highest level while investigators work to sort out what happened. Such an incident would pose an unprecedented challenge for our operations that we have invested and to prevent an incident to work closely with government authorities to restore smooth operations should the system of prevention fail.

Earlier this week, you received testimony from Commander Stephen Flynn. HPH has known Commander Flynn since the year 2000. While he was serving in the U.S. Coast Guard, he spent time studying container operations in our facilities in Hong Kong. Commandeer Flynn at the time was deeply concerned about the rising threat of terrorism and the danger it posed to our industry. Sadly, like so many of the rest of our industry, we did not pay him much heed. After September 11, we listened to Commander Flynn with new respect, realizing along with the vast majority of Americans that the world changed forever that day and we could no longer treat security as an afterthought. We became one of his students versus his teacher, and we looked very closely at the layered approach to security, that being the ISPS Code, inspecting high-risk containers at ports of embarkation, location and tamper evidence monitoring, imaging, and radiation detection.

We believe a layered strategy recognizes that there is no silver bullet to this security and statistically five 60-percent measures when placed in combination will raise the overall probability of success to 99 percent.

HPH has put in place the first layer, the ISPS Code. In the very beginning, we knew that the two initiatives, that with CBP as well as the ISPS Code, did not solve our problem of the Trojan Horse. As a result, we worry that CBP may be overestimating their ability to accurately assess true risk in the industry, because we believe CBP relies on the primary screen of commercially supplied ocean bill of lading/manifest data. And as Secretary Jackson said, it is an excellent first step, and we should be looking forward to the second step.

As a result, only 1 percent of all U.S.-bound containers are actually looked at at the port. The United States, I believe, and the international community should strive to construct a "trust but verify" versus relying just on manifest information.

We have been the lead also in the deployment of radiation detection equipment in the U.K. in Felixstowe as well as deployment of the NNSA program in Rotterdam, and most recently in Freeport, Bahamas.

At HPH we believe it is possible to configure our facilities to support as much high percentage of verifications, and this would come from deploying non-intrusive inspection equipment to examine containers arriving in overseas loading ports to the United States.

When we started the ICIS program, we looked at operating within two of the busiest container ports in the world. Beginning in 2005, every truck entering two of the main gains at Hong Kong International Terminal and Modern Terminal has passed through portal screening technology, and a database of over 1.5 million images has been stored. Key to this pilot is truly the industrial engineering aspect. Many people have discussed here that we are not using them as a radiation alarm or as a scanning tool. We believe that if we could keep the boxes moving versus leaving them to rest, then we could evaluate significantly the NII images with speeds up to 15 kilometers 24 hours a day. The pilot is now being evaluated, I am pleased to say, by DHS/CBP, and they have under review 20,000 containers at this present time.

It was brought up about the illegal aliens that came out of Shenzhen, China, into the port of Los Angeles. If this infrastructure had been deployed 50 miles north, those illegal aliens would have been found. I am pleased to say, though, they were found by the ISPS Code because of the CCTVs and the training of the longshoremen in the facility.

The present focus on ports is long overdue, and we believe that the Congress and the American people need to focus on achievable goals and not become overwrought by their worst fears. But we do believe a "trust but verify" policy, partnering with foreign overseas terminal operators, like my company, that are prepared to come together with an industry Coalition of the Willing. We had that coalition of the willing before some attacks that were in the press, but we feel we can pull that back together again. In fact, the four major container terminal operators loading 80 percent of the containers moving around the globe are headquartered in Hong Kong, Denmark, Dubai, and Singapore.

Since September 11, our company has invested over $200 million to elevate the security in worldwide facilities. John Meredith is exercising, I believe—our CEO—private sector leadership on some-

thing that he believes to be one of our times most urgent global priorities.

Mr. Chairman, I was profoundly moved by the discourse between Governor Kean and Senator Lautenberg on Tuesday when they discussed just when is an issue a priority. We believe this is a global priority and a true issue of priority. Thank you very much.

Senator COLEMAN. Thank you very much, Mr. Gilbert. Mr. Clancey.

TESTIMONY OF JOHN P. CLANCEY,[1] CHAIRMAN, MAERSK, INC., CHARLOTTE, NORTH CAROLINA

Mr. CLANCEY. Thank you, Mr. Chairman. As you may know, Maersk is one of the largest liner shipping companies in the world, serving customers all over the globe. With a fleet numbering more than 500 container and 1.4 million operated containers, the A.P. Moller Group employs 70,000 people in over 125 countries ships.

In the United States and in North America, Maersk Inc. represents A.P. Moller's activities with approximately 12,000 Americans working in our terminals and our offices throughout the country. The businesses we operate today include liner shipping, terminal operations, logistics, warehousing and supply chain operations, and other activities related to the movement of freight.

Maersk has been actively involved in maritime security issues for many years. Our commitment to security is captured by the watch words for the company: "Constant Care." The security of our containers and the integrity of our transportation network are essential to our operations at Maersk. As a worldwide company involved in many places here and abroad, we are constantly aware of the problems of security and safety.

For many years, cargo moved fluidly through our ports and facilities, but certainly that changed with the advent of September 11.

Mr. Chairman, in your letter of invitation, you requested that I address certain specific matters.

Let me begin by commenting on Maersk's perspective on U.S. Government programs related to maritime and port security. Many Federal Government programs are successful. but neither the government nor private industry can achieve maritime security unilaterally. It requires joint efforts. Maersk participates in the Maritime Security Program, which we believe provides a cost-efficient way for U.S. interests to be guaranteed, while at the same time providing benefits to liner companies. In addition, we have entered into a variety of U.S. Government programs and pilot projects. For example, we were the first enterprise-wide transportation company to be validated by C–TPAT.

Maersk also participates in the Super Carrier Initiative, one of approximately 25 ocean carriers working with U.S. Customs and CBP in this area.

Another area of our work with the government involves the issue of employee identification cards, and I was pleased to hear from Secretary Jackson that we're finally moving forward on that.

But we realize that is not enough to make the maritime operations within this country secure, so Maersk has intensified our

[1] The prepared statement of Mr. Clancey appears in the Appendix on page 212.

own efforts through the establishment of a comprehensive security policy and a strategy in this regard.

In short, we agree that maritime security here and abroad can be improved, and we are working cooperatively to achieve this objective, both in partnership with the government and through our own efforts. We have some concerns that government programs not be commercially punitive, duplicative, or inconsistent, or add unnecessary levels of bureaucracy, and that's why the partnership is so important.

You inquired about the use of radiation detection equipment, which has been well spoken and addressed this morning, at seaports and the possible impact to our operations. We have had success in working on this matter with CBP, and we strongly support it.

A third area of inquiry relates to foreign ownership of U.S. terminals. Congressional concern obviously was highlighted with the activities and the possibility of Dubai Ports acquisition in the United States, and also the role of investment in marine terminals in the United States.

A marine terminal operating company typically holds a long-term lease from a public—local or State—port authority to manage the unloading and loading of containers in a marine facility. It is a specialized, highly competitive, low-margin business whose tools—a dock, a crane, and a parking lot—are in the hands of American union labor and American management.

The shipping industry has always been highly globalized and highly competitive. Billions of dollars in foreign investment from the Japanese, South Koreans, Danish, British, Chinese, and others in this country have led to the success of our ability to grow and expand international trade. For example, Maersk alone in the last 3 years has invested $3 billion in U.S. port projects, and we continue to look at other opportunities. Today, foreign-owned companies are running the majority of U.S. marine terminals, as Mr. Koch addressed.

Port authorities prefer large, profitable, predictable volumes that can only be guaranteed by liner companies, so liner-affiliated, foreign terminal operators are the top priority.

Second, liner companies prefer handling their own landside operations because it is the most expensive component of our entire activity chain.

Terminal operators today operate with lease agreements typically awarded and administered by the local governments. There has been no evidence that foreign-controlled companies are less secure, or in any way less compliant with security regulations, or in any way less cooperative with the U.S. Government, particularly on security issues.

Mr. Chairman, your letter also raised the potential impact from a terrorist element smuggling a weapon of mass destruction. I think enough has been said about that this morning, but certainly we are concerned and we believe that more can be done.

Mr. Chairman, finally you asked about specific maritime security recommendations. In general, I would encourage policymakers to evaluate potential programs with an eye toward trade reciprocity. As a carrier that operates in 125 countries around the world, I've

had the experience to see and experience instances in certain ports where it is sometimes a little bit difficult and sometimes very difficult to get them to comply with suggestions. So bilateral agreements, we believe, are mandatory if we are going to be successful, particularly as you want to move towards 100 percent inspections.

Thank you very much.

Senator COLEMAN. Thank you very much, Mr. Clancey. I would mention this Transportation Worker Identification Card is a big deal. And maybe it was you, Mr. Koch, who said that it is probably the most significant thing that can be done right now to enhance the security of the global supply chain. So I was also pleased that we heard the Secretary mention that.

Let me talk a little bit about foreign ownership first. I have some other specific questions, but I wanted to touch upon that first. Mr. Clancey, Maersk, you have an American operation of an international company. Mr. Gilbert, you have an international company that I do not think runs terminals in the United States, but you are centered right here. Maybe Mr. Koch should answer this or maybe you all can.

Would there have been anything—just going back to DP World, Dubai—would there have been anything that would have precluded either economically or operationally from the DP World having an American company, an American operation that would have been subject to vetting by Homeland Security? It probably would have raised, I think, a level of confidence. Is there anything that would have precluded that or made that difficult to happen? We never got to that point.

Mr. KOCH. Other than Congress? And that was the issue. Really, I think Dubai Ports would have been happy to structure that arrangement to put everything that was in the United States in a U.S. corporate structure, as long as, obviously, its ownership interest could be protected. I think they would have been happy to do that. It just got—those kinds of suggestions came up too late to be factored into what became a very active, political issue.

Senator COLEMAN. Anybody else want to respond to that?

Mr. CLANCEY. We have operations very similar to that. One is Maersk Line Limited that operates ships for the U.S. Government. It is a stand-alone company with clearances, and the chairman of that company is the past commander of NATO. They have corporate governance. They have rules and procedures to manage that business as a stand-alone American controlled business, and each year it has examined and validated, and it has always been successful.

Senator COLEMAN. Mr. Gilbert.

Mr. GILBERT. In our case, sir, all of the ports that we have in those countries are incorporated in those countries, so in Panama, let's say we have 1,608 employees. It's a registered company in Panama, but the majority of the shares that are held of that company, in the parent company of HPH. That is repeated in either the Bahamas or Poland or Netherlands of the U.K. It is a question of they are almost exclusively with the country nationals of that country.

Senator COLEMAN. I will ask Mr. Koch and Mr. Clancey this, because it has to do with the Freeport, Bahamas operation. Part of

the Megaports strategy is to work with foreign companies. In fact, it is actually easier to work with foreign companies rather than the foreign country. It is easier to get the level of cooperation, less diplomatic hoops to jump through. Mr. Koch and Mr. Clancey, is there anything that you are aware of in the proposed Megaports situation? We would be working within the Bahamas, in Freeport, with a Hutchison operation, where they would be involved in the Megaports Initiation defense. Is there anything from a security perspective you think would be problematic about that?

Mr. KOCH. Mr. Chairman, I am not aware of anything that's problematic, and one of the things that's encouraging about that particular project is that it examines how you can do the radiation scanning on what remains in the United States an open, unsolved problem, which is, how do you do radiation scanning on boxes that are going onto trains?

The present radiation scanning system in the United States is most easily implemented for boxes going out a gate, and that is fairly easy to set up the screening. There's a lot of cargo that leaves U.S. ports via on-dock rail. The Port of Tacoma, for example, has been struggling with this. The project in the Bahamas is testing and using a technology that can be put on container handling equipment that maybe can answer the question of how to efficiently screen containers being moved onto on-dock rail and could also help maybe be applied in the United States as well.

Senator COLEMAN. Mr. Clancey.

Mr. CLANCEY. I don't see any problems whatsoever. Our only concern is the real-time use of that information, that the instant that it's scanned, within a very short period of time before that container is fluid in our yards, that we're told it's a "no go." We can't make those decisions. We simply can't call the shipper and say, "We're not going to move your container because we have a concern." But if the government and Homeland Security can develop a message, working with Customs, to give us immediate alerts, we don't see any issues at all.

Senator COLEMAN. I am not going to ask you, Mr. Gilbert, since you got a dog in that house.

Mr. GILBERT. Could I make a comment on the technology though, sir?

Senator COLEMAN. Please.

Mr. GILBERT. NNSA brought in a technology that does a primary scan and a secondary scan with an isotope. We have taken and put this operation where we have dropped the alarm down to the bottom. We have approximately, at this present time, about 25 percent rate of alarms. And then we do a secondary scan. The first scan goes at seven kilometers, the second scan at three kilometers. And we have, because with the containers at risk, we have a very good scan. Whereas, in Hong Kong, we've turned the alarm bells off because this is a proof of concept, but we have stored the images as well as the radiation signatures, and they are available on our disk.

Senator COLEMAN. One of the questions I have, maybe it is a question about technology, one of the concerns—and I think the figure was 4 to 6 minutes. I forgot who raised that. I think Mr. Koch. You talked about how it takes 4 to 6 minutes for a trained expert

to actually analyze the image, and say what is in there. Looking to the future, my sense would be that computer programming using different algorithms would be able to cut that substantially. Is there anything on the horizon with this technology?

Mr. KOCH. We understand that a number of people are working exactly on that, but it does require matching an understanding of the contents of the container with the image though, which is going to require systems integration. Hopefully, that could be done. On some commodities, let's say it's a light commodity like apparel or footwear, anomalous images are probably very easy to identify if there is something here that causes a question. On high-density cargoes, auto parts, machine parts, things like that, it's going to be a difficult and more serious challenge. But we know, in talking with SAIC and other vendors, that they are working assiduously on trying to develop software that could be used by the government in a reliable way.

Senator COLEMAN. Because the issue here really is security. That is our concern. Yours is security but also speed. You have to make a profit, and those things that slow it down become problematic. Through some technology, such as ICIS, speed has not been compromised. I just do not want the bureaucrats to come back and say it takes 4 to 6 minutes when I have to believe that you have some computer technology that will allow you to do analysis very quickly. The key here again is to highlight those things that are high risk should be scanned at a minimum.

Mr. Clancey, you talked about the bilateral agreements that work in other countries. Senator Levin's question, and then my follow-up question, what if the United States simply said to folks in Japan, or in Hong Long, or LeHavre, or somewhere else, "We are not allowing stuff to go out if it has been identified high risk without there being some further level of review." Would that present any economic problems, any issues with that?

Mr. CLANCEY. I think that if you had the scanners, if we had a system that we were comfortable with, and if we had the ability to interpret the data in real time and Customs reaches a conclusion that there's an issue here. I've worked and lived in a lot of countries around the world. I think that if the shipment was held for 1 hour, 2 hours, or 6 hours, it wouldn't be an issue.

Senator COLEMAN. Mr. Koch.

Mr. KOCH. In listening to the conversation between yourselves and Mr. Jackson, I was struck by the question of whether or not there is some ambiguity on the term "high risk." There are certainly some things that Customs is going to really want to take a close look at and inspect the container, where it's probably perfectly OK to do that in the U.S. port, if it's contraband, for example, if it's drugs, if it's those kinds of things.

If, on the other hand, the government actually believes that there's a high risk that this box contains a terrorist potential, that should never be allowed to be loaded onto a ship and be brought to the United States.

So I think the term "high risk" is used to describe a whole list of things that get triggered in their automated targeting system, some of which clearly require inspection in the foreign port, and some of which are probably perfectly OK to let in, and then you

refuse to release the box at the U.S. port until it's gone through the inspection process. I think maybe some analysis in coming up with a clear definition of "high risk" might handle——

Senator COLEMAN. My problem is I am a former prosecutor, Mr. Koch, and I have a kind of philosophy that bad guys tend to hang out with bad guys, and if somebody is in the drug and human trafficking business, and I offered him another $50,000 or $100,000 to transport this other piece of cargo, I do not think there would be any moral fiber that would say, I should worry about that. And that is why if it is high risk, I think we got to take a look at it.

Mr. KOCH. I don't think there's an ocean carrier out there that would object to the U.S. Government saying, "Do not load any box the U.S. Government thought was a high-risk box."

Mr. CLANCEY. If I could add to that, Mr. Chairman, just so that you have a frame of reference to discuss this with your colleagues. In the peak, that's the busiest time of our year, each day thousands of boxes are rolled, and the roll means they're left behind. They're left behind because there's no space on the ship. So physically it's very easy to do, and sometimes it's a matter of policy.

Senator COLEMAN. Mr. Clancey, you said at one point you believe we are doing good things but believe more can be done. And my last question before I turn to the Ranking Member is, what more can be done? What are we not doing we should be doing? And I would like each of you gentleman to address that.

Mr. CLANCEY. I think that speed and velocity is terribly important. I mean I was not only pleased with Secretary Jackson's comments, I was surprised. But I think it is that type of speed execution that is terribly important. There's a lot of things being looked at, maybe there's 100, but there's probably 5 or 10 you could prioritize, implement, and even if they're not 100 percent perfect at this time, put them in place.

Senator COLEMAN. And I would like to work with you further for you to identify those 5 or 10. We would like to know what the private side is saying and then see if government can move forward.

Mr. Gilbert.

Mr. GILBERT. Sir, I think one of the things that came out of DP World was the education of the American people, but some way, I think that went astray a little bit to fear-mongering as well. I think that this dialogue that you are having right now about where we are with foreign ownership, I think that needs to be explored more. And the public-private partnership is what's going to come from that, but if there's a fear side to having a public-private partnership with those that have headquarters in Denmark or Singapore, then that's going to be a very difficult thing.

We are going to continue to put money into security because it is good for our industry, and the leader of our company believes that as an industry leader, that we must do that. But we need that to be embraced and worked with as we go forward in these pilots. Thank you, sir.

Senator COLEMAN. Mr. Koch.

Mr. KOCH. I would agree with Mr. Gilbert and Mr. Clancey's comments. The only things I would add is in terms of priorities, first, the focus again on ICIS. How can it be integrated as another tool in the toolbox? That obviously means working with Customs

very closely on developing acceptable operating protocols and agreements with foreign governments, because this is international trade and we can expect foreign governments to expect reciprocity. We can't just expect everybody in the world to do what we want in their ports without us being willing to do the same thing in our ports for our export cargo.

Second, the TWIC, we are looking forward to seeing this move forward.

But third, again, to emphasize that it is important in our view to improve the data used for cargo risk assessment. Our strategy today is based on risk assessment, and the data being used is good but it is limited. The Secure Freight Initiative that DHS has spoken about as a next-generation strategy, is exceptionally ambitious as described, involving great quantities of data from great quantities of people, potentially going to third party commercial sources before being used by the government. That's a wonderful vision, and it's a great vision, but it's a very ambitious agenda. We would hope that the government would not wait until that is ready to be rolled out before we take the next generation of improvement.

Frankly, today, our customers give the government no data that can be used in the before-vessel-loading screening process, and we think that ought to be addressed because there are too many holes that could be easily closed by either the customer's entry data being provided, just as the carrier's entry data is provided, or other data elements that perhaps the government would want. That data should be given to CBP 24 hours prior to vessel loading, so that the strategy we have embarked upon of doing the risk assessment before vessel loading can be matured into something that we could all have more confidence in.

Senator COLEMAN. Very helpful, Mr. Koch. Thank you.

Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman.

I think one of you made reference to the percentage of American ports that are operated by foreign companies. Was that you, Mr. Koch?

Mr. KOCH. It's a substantial majority of the terminal operations being run by companies that are foreign-owned companies, yes.

Senator LEVIN. What percentage of the terminal operations are owned by foreign companies in Japanese ports?

Mr. KOCH. I don't know the answer to that.

Senator LEVIN. What would your guess be?

Mr. KOCH. The majority will be Japanese. I remember when——

Mr. CLANCEY. 100 percent are Japanese.

Senator LEVIN. I think that is——

Mr. CLANCEY. But that's something the U.S. Government has been involved in for a long time.

Senator LEVIN. Been involved in allowing that?

Mr. CLANCEY. Trying to break that monopoly.

Senator LEVIN. Yes, but we have not, have we?

Mr. CLANCEY. We have not. That's the only country in the world probably where the monopoly hasn't been broken.

Senator LEVIN. What are you guys going to do about that? Do you believe in foreign trade, foreign ownership—Mr. Koch, you are

the head of the World Shipping Council. Are the Japanese part of that?

Mr. KOCH. Yes, they are.

Senator LEVIN. What do they say when they are told, hey, you guys do not allow foreign ownership at your ports?

Mr. KOCH. They went through an experience several years ago with the Federal Maritime Commission pursuing that quite aggressively, and several years ago, when I worked for Mr. Clancey and we were all at Sealand together, we worked very hard to try to get into the Japanese ports, and it's a difficult problem.

Senator LEVIN. Why do we tolerate it? Why do you tolerate it? Why don't you kick them out of your council?

Mr. KOCH. I think the shipping lines that are members of the council are responsible operators.

Senator LEVIN. We talk about aggressive, but it is hitting your head against the wall if it does not succeed, and I find this such a one-way street. It is so typical of trade, as far as I am concerned. We look at our trade imbalance. Part of it is obviously caused by reasons of cheaper labor and a lot of other things, but part of it is just caused by closed markets to us, and if you want to hold up foreign ownership of ports as being part of a global economy, or port facilities here as being part of a global economy, it seems to me unless the private sector joins our government in trying to open up the Japanese or any other country that closes their market to us, it is going to continue to be a far different situation than a two-way street in trade.

I do not know what more I can add on that subject, other than to tell you I am not particularly sympathetic in terms of the foreign ownership issues until all the countries who do trade with us, particularly these countries that have huge balances with us, positive trade balances with us, live by the same rules we do.

So you can pass that angst along, and add it to a long list.

Mr. CLANCEY. Yes, Senator, but it's also true that almost every other country in the world allow foreign companies to operate their ports and——

Senator LEVIN. How about the Chinese?

Mr. CLANCEY. Yes.

Senator LEVIN. So what percentage of Chinese port facilities are owned by foreign interests? Do you know offhand?

Mr. CLANCEY. Foreign investments, I'd say 30.

Mr. GILBERT. Well, if you consider Hong Kong——

Senator LEVIN. No, skip Hong Kong. Are you including Hong Kong, Mr. Clancey?

Mr. CLANCEY. No, I'm not including Hong Kong.

Senator LEVIN. You think it is 30 percent outside——

Mr. CLANCEY. I would say that of the container activities between the Singaporeans, ourselves, Europeans, a lot of private capital venture funds, maybe 25 to 30.

Senator LEVIN. And how about South Korea, are they open?

Mr. CLANCEY. Yes.

Senator LEVIN. So a significant percentage of their facilities would be owned by foreign interests?

Mr. CLANCEY. Not a significant amount, but there's no limitations.

Senator LEVIN. And no practical limitations either, OK. There is not barriers which are——

Mr. CLANCEY. No.

Mr. GILBERT. What has happened, Senator, is a number of countries have gone and privatized their ports because they're looking for private capital to come in. If you look at all of the investment that's gone into Korea in the past, it had been U.S. investment that turned into DPW investment when that was sold, significant investment from Hong Kong and significant investment from Singapore.

If you look at the U.K., all of their ports are privatized. We operate about 60 percent of it in the north, and P&O Ports, now DPW, operates in the south. And that goes around the globe. Actually, capital goes where it's treated well, and in privatizations it is treated well.

Senator LEVIN. How about Dubai in the Emirates, are their ports privately—their operations are owned by foreigners too?

Mr. CLANCEY. Correct.

Mr. GILBERT. I would point out though, Senator, an interesting fact, that when Jebel Ali, the biggest port in the Middle East, was——

Senator LEVIN. Where is that?

Mr. GILBERT. In Dubai. Was constructed, for the first 10 years an American company ran that facility. And I know that because I was the first port director of that facility. And then they learned how to run their own facilities, and then they took them over, and in the past 2 years, have been expanding greatly into terminal operations.

Senator LEVIN. Are they currently owned by a foreign interest in Dubai or the Emirates?

Mr. GILBERT. I believe they are all owned by Dubai Port World now. If we go to other places such as Salalah, Denmark, A.P. Moller has a big facility there, and we have just bought one in Oman as well, SLR.

Senator LEVIN. Twenty-four million containers come into the United States each year, 11 million by sea, 11 million by truck, 2 million by train, according to the figures I have used. I assume those are all filled containers?

Mr. KOCH. For ocean, the inbound trade is generally filled, yes.

Senator LEVIN. And how about going out?

Mr. KOCH. A lot of air.

Senator LEVIN. A lot of empty containers?

Mr. KOCH. A lot of empties.

Senator LEVIN. What percentage of the containers that leave the United States leave empty, by sea?

Mr. KOCH. I believe there's about 7 million export containers, and I believe between 6½ and 7 million. I can check that figure for you.

Senator LEVIN. That go back loaded?

Mr. KOCH. Loaded.

Senator LEVIN. So half are loaded, half of them empty.

Mr. KOCH. The carrier will have to reposition the empty from here back to Asia to pick up a load, so that you always have to maintain equipment balance.

Senator LEVIN. But would you say that of the 11 million coming by ocean into the United States, perhaps half go back somewhere empty?

Mr. KOCH. Probably not quite that high, but it's certainly a large percentage.

Senator LEVIN. Forty to 50 percent?

Mr. KOCH. Forty percent is probably getting close.

Senator LEVIN. Would you know the figure by truck? Would any of you have an idea by truck?

[No response.]

Senator LEVIN. OK. I think, Mr. Koch, you said it would be wrong for Congress to restrict foreign investment in any way in our port facilities. Do you consider that the law that we have on the books currently, which requires a 45-day formal investigation where there is an allegation that a transfer could affect the national security of the United States, do you consider that to be an inappropriate restriction?

Mr. KOCH. No, sir.

Senator LEVIN. Mr. Gilbert, you talked about ICIS, and I am interested as to whether or not there is any other similar technologies being developed, or is ICIS kind of by itself there?

Mr. GILBERT. It was an engineering and proof-of-concept study, and we have told all the vendors that just as we build cranes and buy cranes, that we don't have a specific vendor. So we think that if this is accepted, that images as well as radiation screening, then we will have the start of a market that many vendors will come into, both lowering the cost and increasing the capabilities and ability to do better scans and better radiation detection.

Senator LEVIN. So those others at that point will be able to utilize those technologies? They are not patented or not——

Mr. GILBERT. The key is that the radiation portal can be pretty much interchanged. The one on the scan, the uniqueness of the vendor that has provided to us, is able to open a shutter and close a shutter as a truck moves through. So they have that pretty much now as a prototype that others have not done. Once that somebody knows there's a market for it, they will be building it quickly.

Senator LEVIN. You think then there will be competitors?

Mr. GILBERT. We absolutely will request competitors for sure.

Senator LEVIN. Mr. Gilbert, there have been allegations about the relationship between your company and the Chinese Government. Is there any relationship, and if so, what is it?

Mr. GILBERT. We are a publicly traded company, and we have been since we started as the No. 1 company in 1866, with a handover and reversion in 1997. We became part of a SAR, and the whole Hong Kong——

Senator LEVIN. What is an SAR?

Mr. GILBERT. The Special Administrative Region of China.

Senator LEVIN. OK.

Mr. GILBERT. And the Hong Kong Exchange fell within that. An interesting side, we have HPH is talked about, but actually, HSBC, the first director of HPH went to HSBC, the bank, and they're there. We've got a particular note because of the fact that we have a lot of investment in China, but we have no government shares in our company whatsoever.

Senator LEVIN. So the government has no connection to your company?

Mr. GILBERT. Well, we certainly are good citizens in every country——

Senator LEVIN. I know that, but in terms of ownership or control.

Mr. GILBERT. There is no ownership or control, sir.

Senator LEVIN. Thank you. My time is up. Thank you very much. Thank you all.

Senator COLEMAN. Thank you, gentlemen. It has been a very informative, very helpful panel, and we are very appreciative, so thank you much.

With that, this hearing is adjourned.

[Whereupon, at 12:25 p.m., the Subcommittee was adjourned.]

APPENDIX

PREPARED STATEMENT OF SENATOR AKAKA

MARCH 30, 2006

Thank you, Mr. Chairman. I commend you for holding this series of hearings on the critically important issue of securing our global supply chain.

As you know, cargo security is especially important to my state of Hawaii because we receive 98 percent of imported goods via the sea. Any interruption in sea commerce would have a staggering impact on the daily lives of the people in Hawaii.

We must do everything possible to ensure supply chain security while enabling and not impeding trade. This balancing act is critical—with no room for error. Programs such as the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) are part of that balancing act.

CSI and C-TPAT have improved global supply chain security, but have not yet perfected supply chain security. Our vulnerabilities remain high, and there are considerable areas for improvement. These programs use voluntarily submitted information to focus scarce screening resources and target high-risk shippers and cargo. While all cargo is reportedly screened, only five percent is targeted for inspection.

Both the Government Accountability Office (GAO) and the Department of Homeland Security's Inspector General have reported glaring weaknesses with Customs and Border Protection's (CBP) targeting methodology and execution. This targeting methodology, which forms the backbone of our present inspection process and plays a critical role in combating nuclear and radiological smuggling efforts, must be improved.

To strengthen our targeting efforts, CBP must also ensure the nation's intelligence community is sharing counter-terrorism information to strengthen targeting methodologies. Although the number of ports participating in CSI and C-TPAT continues to grow, the number of CBP inspectors has not risen correspondingly. Because of CBP's inability to fully staff some ports, 35 percent of shipments are not targeted and, therefore, not subject to inspection overseas. GAO pointed out nearly a year ago these staffing imbalances and shortfalls.

But, Mr. Chairman, it is not only GAO who has expressed concern over staffing. I've been contacted by the National Treasury Employees Union (NTEU) because of their concern over a decrease in staffing levels. Without a sufficient number of trained inspectors, how can we expect our borders to be protected? More troubling, the President's Budget for fiscal year 2007 requests an increase of only $32 million and 21 full-time employees for all CBP operations at ports of entry. This stands in contrast with other human capital initiatives within the Department, including a $41.7 million or 133 percent increase for funding MaxHR, the new personnel system at DHS. I question the Administration's commitment to address these critical staffing problems within CBP.

As I've discussed before, I am also concerned about the potentially duplicative programs in the newly established Domestic Nuclear Detection Office (DNDO) and the National Nuclear Security Administration in the area of radiation detection technologies. These technologies must used effectively within the framework CSI and C-TPAT. Detection technologies must also be effective at detecting and deterring nuclear or radiological materials while also expediting the flow of commerce. The new DNDO runs the risk of becoming another layer of bureaucracy on a crowded organizational chart, duplicating technologies being developed elsewhere in the federal government, and siphoning off scarce science and technology funds from other programs. Thank you, Mr. Chairman.

Prepared Statement of
The Hon. Thomas H. Kean
Former Governor, State of New Jersey
Former Chair of the National Commission on Terrorist Attacks Upon the United States
before the
Permanent Subcommittee on Investigations
Committee on Homeland Security and Government Affairs
United States Senate
March 28, 2006

Mr. Chairman, Senator Levin, distinguished members of the Permanent Subcommittee on Investigations, it is an honor to appear before you today. This subcommittee, under both its past and current leadership, has made a profound contribution to the national security of the United States.

Your investigative and oversight work on the question of the safety, secure storage, and interdiction of nuclear materials continues to be a vital part of the nation's non-proliferation efforts. I commend this Committee for its leadership.

Mr. Chairman, the National Commission on Terrorist Attacks Upon the United States, (better known as the 9/11 Commission) made 41 recommendations when it issued its report in July, 2004.

We think each of those recommendations is important. The ten former Commissioners worked very hard this past year to get those recommendations written into law and implemented into action. We made some useful progress, but a lot of work remains to be done.

The Most Important Recommendation

Of all our recommendations that need attention, *surely the most important* is to prevent terrorists from gaining access to nuclear weapons. These are the weapons Usama bin Laden has promised to get and to use.

We know that he has been working to acquire them for more than a decade, as we document in our report. We know that he has been scammed by con artists, but we know he keeps trying.

Testifying in a Federal courtroom in early 2001, an al-Qaeda member explained his mission: "it's easy to kill more people with uranium." We known bin Laden's intent. We know he is patient. We know he plans carefully.

We do not think that a nuclear attack is the most likely event. Attacks of the kind we saw in Madrid and London mark the more likely pattern. But a nuclear event is possible, and it would have profound and incalculable consequences.

It would put millions of lives at risk. It would devastate our economy and way of life. It must be elevated above all other problems of national security, because it represents the greatest threat to the American people.

The Commission's report could not be more clear: "preventing the proliferation of these weapons warrants a maximum effort...."

How Are We Doing?

So how are we doing? What progress are we making against the proliferation threat? What progress are we making keeping weapons out of the hands of terrorists?

The Commission believed, as I know Senator Nunn believes, that it is most important to secure nuclear materials at their source. The Cooperative Threat Reduction Program, better known as the Nunn-Lugar program, is carrying out important and useful actions to secure nuclear materials at their source, and in some cases to transport materials to more secure locations.

People in government – especially at the Defense, State and Energy Departments – are working hard to implement these programs. I commend them for their important work.

On the policy front there are some positive signs.

-- President Bush and President Putin made an agreement in Bratislava last year, and it gave the bureaucracy a push.

-- American inspectors now have additional access to weapons storage sites in Russia.

-- Liability issues—which had delayed efforts to eliminate plutonium from dismantled weapons—seem to be getting resolved.

-- More of the vulnerable nuclear facilities in Russia are receiving security upgrades

-- The current Defense Authorization Act includes amendments by Senator Lugar that cut bureaucratic red tape and will speed up the work of the Nunn-Lugar program.

These are good steps. But they are not nearly enough.

What is most striking to us is that the size of the problem still totally dwarfs the policy response:

-- The Nunn-Lugar program to secure nuclear materials in the former Soviet Union is 14 years old. About half of the nuclear materials in Russia still have no security upgrades whatsoever.

-- At the current rate of effort, it is going to take another 14 long years to complete the job. Is there anybody anywhere who thinks we have 14 years?

-- This is unacceptable. Bin Laden and the terrorists will not wait. The challenge is bigger than the former Soviet Union:

  o Some 40 countries have the essential materials for nuclear weapons.

  o Well over 100 research reactors around the world have enough highly-enriched uranium present to fashion a nuclear device.

- o Too many of these facilities lack any kind of adequate protection. The terrorists are smart. They will go where the security is weakest.

Our own agencies need to make protecting the nation from a possible WMD attack an absolute priority. We are disappointed to hear, for example, that the FBI is not further along on preventing weapons of mass destruction.

In short, we still do not have a maximum effort against what everybody agrees is the most urgent threat to the American people.

When is an issue a priority?

Everyone knows when an issue is the highest priority. It is a priority when our leaders are talking about it.

-- Why isn't the President talking about securing nuclear materials?

-- Apart from the superb efforts of this Committee, why isn't the Congress focused? Why aren't there more hearings and greater Member interest?

-- What about the media? Why aren't the airwaves filled with commentary if everyone agrees that the crossroads of terrorism and nuclear weapons is the most serious threat to our security?

Next Steps

The President should develop a comprehensive plan to dramatically accelerate the timetable for securing all nuclear weapons-usable material around the world.

He should request the necessary resources to complete this task.

He should publicly make this goal his top national security priority, and ride herd on the bureaucracy to maintain a sense of urgency.

The Congress should provide the resources needed to secure vulnerable materials at the fastest possible rate.

The Congress should work with the President to build public support for this effort.

The President and the Congress need to work together on a bipartisan basis. There is simply no higher priority on the national security agenda.

#

COUNCIL ON FOREIGN RELATIONS

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

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

Written Testimony before

a hearing of the

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

on

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

by

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

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

9:30 a.m.
March 28, 2006

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

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

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

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

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

A container of athletic foot wear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.

The driver takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship which typically carry 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ships goes to Hong Kong where it is loaded on a super-container ship that carriers 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. Because it originates from a trusted-name brand company that has joined the Customs-Trade Partnership Against Terror, the shipment is never identified for inspection by the Container Security Initiative team of U.S. customs inspectors located in Vancouver. Consequently, the container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a railyard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.

There would be four immediate consequence associated with this attack. First, there would be the local deaths and injuries associate with the blast of the conventional explosives. Second, there would be the environmental damage done by the spread of industrial-grade radioactive material. Third, there would be no way to determine where the compromise to security took place so the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Fourth—and perhaps most importantly—all the current container and port security initiatives would be compromised by the incident.

In this scenario, the container originated from a one of the 5,800 companies that now belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been certified by their host nation as compliant with the post-9/11 International Ship and Port Facility Security (ISPS) Code that came into effect on 1 July 2004. Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors in Hong Kong or Vancouver. Nor would it have been identified by the radiation portal. As a consequence, governors, mayors, and the American people would have no faith in the entire risk-management regime erected by the administration since 9/11. There will be overwhelming political pressure to move from a 5 percent physical inspection rate to a 100 percent inspection rate, effectively shutting down the flow of commerce at and within our borders. Within two weeks, the reverberations would be global. As John Meredith, the Group Managing Director of Hutchison Port Holdings, warned in a Jan 20, 2004 letter to Robert Bonner, the former Commissioner of the U.S. Customs and Border Protection: **". . . I think the economic consequences could well spawn a global recession – or worse."**

In short the stakes are enormous. But there are four factors associated with the scenario that I just laid out that usefully informs the focus of this hearing. First, the threat is not so much tied to seaports and U.S. borders as it is global supply chains that now largely operate on an honor system because the standards are so nominal. Second, no transportation provider, port operator, or border inspector really know what are in the

containers that pass through their facilities and the radiation portal technology currently being deployed at U.S. borders and as a part of the Second Line of Defense and Megaports programs can be evaded by placing light shielding around a weapon. Third, private companies must be a part of the solution since they have huge investments at stakes. Fourth, the scenario I just laid out involved Vancouver as the offload port in North America, highlighting that the challenge of securing global supply chains can involve both port security and border security measures simultaneously.

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

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

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

Against this strategic backdrop, I believe there remains too little appreciation within the U.S. government that global supply chains and the intermodal transportation system that supports them remains a very vulnerable critical infrastructure to mass disruption. Instead, U.S. border agencies and the national security community have been looking at supply chains as one of a menu of smuggling venues. Some agencies like the Coast Guard and the Office of Naval Intelligence has argued that a weapon of mass destruction

is more likely to be smuggled into the United States on a fishing vessel, ocean-going yacht, or a bulk cargo vessel, rather than in a container. This is probably an accurate assumption in the case of a nuclear weapon. A nuclear weapon would be such a high-value asset to a terrorist organization that they would be unlikely to surrender custody of it to unwitting third parties to transport it. But the opposite reason applies to a "dirty bomb" which is more commonly referred to by national security experts as a "weapon of mass disruption" because its lethality is fairly limited, a factor primarily of the conventional explosives with which it is made. The radioactive material contained in the bomb would create costly environmental damage and potentially some long term health risks for those who were exposed, but not immediate deaths. The fact that a "dirty bomb" is suited for *disruption* makes it an ideal weapon to set off within the intermodal transportation system, precisely because it would generate the kinds of consequences that my scenario portends.

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

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

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

The U.S. Customs and Border Protection Agency (CBP) has pursued a mix of unilateral, bilateral, and multilateral approaches. First, U.S. customs authorities mandated that ocean carriers electronically file cargo manifests outlining the contents of containers

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

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

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

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

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

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

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

Prior to 9/11, the cornerstone of the risk assessment framework used by customs inspectors was to identify "known shippers" that had an established track record of being engaged in legitimate commercial activity and playing by the rules. Since 9/11, the agency has built on that model by extracting a commitment from shippers to follow the

supply chain security practices outlined in the Customs-Trade Partnership against Terrorism (C-TPAT). As long as there is not specific intelligence to tell inspectors otherwise, shipments from C-TPAT companies are viewed as presenting little risk.

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

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

Second, terrorists are likely to find it particularly attractive to target a legitimate company with a well-known brand name precisely because they can count on these shipments entering the United States with a only a cursory look or no inspection at all. It is no secret which companies are viewed by U.S. customs inspectors as "trusted" shippers. Many companies who have enlisted in C-TPAT have advertised their participation in press releases or with postings on their website. In public speeches, senior U.S. customs officials have singled out several large companies by name as model participants in the program. So all a terrorist organization need do is to find a single weak link within a "trusted" shipper's complex supply chain, such as a poorly paid truck driver taking a container from a remote factory to a loading port. They can then circumvent the mechanical door seal and gain access to the container in one of the half-dozen ways well-known to experienced smugglers. Since inspectors view past performance as the primary indicator of current and future compliance, as long as the paperwork is in order, the compromised cargo container almost certainly will be cleared to enter a U.S. port without anyone ever looking at it.

There is third important reason why terrorists would be more willing than criminals to exploit the supply chains of well-established companies. By doing so, they can count on generating far greater economic disruption. This is because once a dirty bomb arrives in the United States via a trusted shipper, the risk management system that customs authorities are relying on will come under withering scrutiny. In the interim, it will

become politically impossible to treat cross-border shipments by other trusted shippers as low risk. When every container is assumed to be potentially high risk, everything must be examined which translates into putting the intermodal transportation system into gridlock.

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

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

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

In the end, the container security measures being pursued by the U.S. government resembles a house of cards. In all likelihood, when the next terrorist attack occurs on U.S. soil and it involves a maritime container it will have come in contact with most or even all the these new security protocols. That is, the container likely will be from a C-TPAT company. It will have originated or been transshipped through a CSI port. It will

have been handled in an ISPS compliant marine facility and crossed the ocean on an ISPS complaint ship. It will have passed through a radiation portal and gone undetected. As a consequence, when the attack happens, the entire security regime will implicated generating tremendous political pressure to abandon it.

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

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

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

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

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

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

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

From the standpoint of U.S. security, the biggest value of this system should it be widely deployed are twofold. First, it provides a powerful deterrent to discourage terrorists from *exploiting* global supply chains as a conduit for a weapon of mass destruction. This importantly also includes its counterproliferation potential. If such a system were in place in the terminals owned and operated by Hutchison Port Holdings and Dubai Port World in the port of Karachi Pakistan, it would make that port a far less attractive place through which to smuggle nuclear materials to the Middle East. The same holds true of ports along coastal China near North Korea. Second, it creates a powerful deterrent to discourage terrorists from *targeting* the global supply chains with a "dirty bomb" since

the inspection system will make the intermodal system far more resilient in managing a breach of security without a wholesale shutdown of the trade system.

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

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

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

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

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

At the end of the day, confronting the nuclear smuggling threat requires that we take the post-9/11 security framework the U.S. government has been developing largely on the fly over the past four years, and quickly move it to the next generation of initiatives that build on the original framework. We have a version 1.0. We need a version 2.0. The three key ingredients of getting from where we are to where we must be are: (1) to

recognize that it is a global network that we are trying to secure; (2) that much of that network is owned and operated by private entities, many who have foreign ownership so U.S. government must be willing and able to work with those companies as well as their host governments so as to advance appropriate safeguards, and (3) both Congress and the White House should embrace a framework of "trust but verify," in President Ronald Reagan's phrase, based on real global standards and meaningful international oversight.

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

Stephen Flynn is the author of *America the Vulnerable.* He is currently writing a new book to be published by Random House in Fall 2006 entitled, *The Edge of Disaster: Catastrophic Storms, Terror, and American Recklessness.* He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report "*America: Still Unprepared—Still in Danger*," co-chaired by former Senators Gary Hart and Warren Rudman. Since 9/11 he has provided congressional testimony on homeland security matters on fifteen occasions. He spent twenty years as a commissioned officer in the U.S. Coast Guard including two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issues on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.

United States Government Accountability Office

GAO

Testimony

Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EST
Tuesday, March 28, 2006

COMBATING NUCLEAR SMUGGLING

Challenges Facing U.S. Efforts to Deploy Radiation Detection Equipment in Other Countries and in the United States

Statement of Gene Aloise, Director
Natural Resources and Environment

GAO-06-558T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-558T, a testimony before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

GAO is releasing two reports today on U.S. efforts to combat nuclear smuggling in foreign countries and in the United States. Together with the March 2005 report on the Department of Energy's Megaports Initiative, these reports represent GAO's analysis of the U.S. effort to deploy radiation detection equipment worldwide.

In my testimony, I will discuss (1) the progress made and challenges faced by the Departments of Energy (DOE), Defense (DOD), and State in providing radiation detection equipment to foreign countries and (2) the Department of Homeland Security's (DHS) efforts to install radiation detection equipment at U.S. ports of entry and challenges it faces.

What GAO Recommends

In the report on U.S. efforts to combat nuclear smuggling in other countries, GAO made five recommendations to improve, among other things, equipment maintenance, coordination among U.S. programs, and accountability of equipment. Both DOE and State agreed with GAO's recommendations. In the report on radiation detection at U.S. ports of entry, GAO made nine recommendations designed to help DHS speed up the pace of portal monitor deployments, better account for schedule delays and cost uncertainties, and improve its ability to interdict illicit nuclear materials. DHS agreed with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-558T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gene Aloise at (202) 512-3841 or aloisee@gao.gov.

March 28, 2006

COMBATING NUCLEAR SMUGGLING

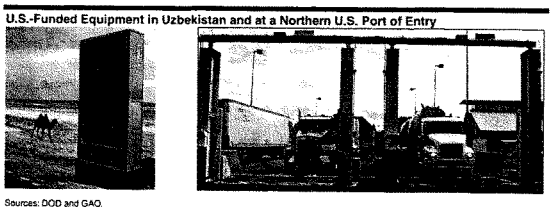
Challenges Facing U.S. Efforts to Deploy Radiation Detection Equipment in Other Countries and in the United States

What GAO Found

Regarding the deployment of radiation detection equipment in foreign countries, DOE, DOD, and State have spent about $178 million since fiscal year 1994 to provide equipment and related training to 36 countries. For example, through the end of fiscal year 2005, DOE's Second Line of Defense program had completed installation of equipment at 83 sites, mostly in Russia. However, these agencies face a number of challenges that could compromise their efforts, including corruption of foreign border security officials, technical limitations and inadequate maintenance of some equipment, and the lack of supporting infrastructure at some border sites. To address these challenges, U.S. agencies plan to take a number of steps, including combating corruption by installing multitiered communications systems that establish redundant layers of accountability for alarm response. State coordinates U.S. programs to limit overlap and duplication of effort. However, State's ability to carry out this role has been limited by deficiencies in its interagency strategic plan and its lack of a comprehensive list of all U.S. radiation detection equipment provided to other countries.

Domestically, DHS had installed about 670 radiation portal monitors through December 2005 and provided complementary handheld radiation detection equipment at U.S. ports of entry at a cost of about $286 million. DHS plans to install a total of 3,034 radiation portal monitors by the end of fiscal year 2009 at a total cost of $1.3 billion. However, the final costs and deployment schedule are highly uncertain because of delays in releasing appropriated funds to contractors, difficulties in negotiating with seaport operators, and uncertainties in the type and cost of radiation detection equipment DHS plans to deploy. Overall, GAO found that U.S. Customs and Border Protection (CBP) officers have made progress in using radiation detection equipment correctly and adhering to inspection guidelines, but CBP's secondary inspection procedures could be improved. For example, GAO recommended that DHS require its officers to open containers and inspect them for nuclear and radioactive materials when they cannot make a determination from an external inspection and that DHS work with the Nuclear Regulatory Commission (NRC) to institute procedures by which inspectors can validate NRC licenses at U.S. ports of entry.

U.S.-Funded Equipment in Uzbekistan and at a Northern U.S. Port of Entry



Sources: DOD and GAO

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our work on U.S. government programs to combat nuclear smuggling through the deployment of radiation detection equipment at border crossings and other ports of entry both in foreign countries and in the United States.[1] According to the International Atomic Energy Agency, between 1993 and 2004, there were 662 confirmed cases of illicit trafficking in nuclear and radiological materials worldwide. Twenty-one of these cases involved material that could be used to produce a nuclear weapon, and over 400 involved materials that could be used to produce a device that uses conventional explosives with radioactive material (known as a "dirty bomb"). Especially in the aftermath of the attacks on September 11, 2001, there is heightened concern that terrorists may try to smuggle nuclear material or a nuclear weapon into the United States. This could happen in several ways: nuclear materials could be hidden in a car, train, or ship; sent through the mail; carried in personal luggage through an airport; or walked across an unprotected border. If terrorists were to accomplish this, the consequences could be devastating to our national and economic interests.

In response to these threats, four U.S. agencies, the Departments of Energy (DOE), Defense (DOD), State (State), and Homeland Security (DHS), implement programs to combat nuclear smuggling in foreign countries and in the United States. Regarding U.S. efforts in other countries, the first major initiatives to combat nuclear smuggling during the 1990s concentrated on deploying radiation detection equipment at borders in countries of the former Soviet Union. One of the main U.S. programs providing radiation detection equipment to foreign governments is DOE's Second Line of Defense program, which began installing equipment at key sites in Russia in 1998. In 2003, DOE began a second program, the Megaports Initiative, to combat nuclear smuggling at major

[1]See GAO, *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain*, GAO-06-389 (Washington, D.C.: Mar. 22, 2006) and *Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries*, GAO-06-311 (Washington, D.C.: Mar. 14, 2006).

foreign seaports.[2] In addition to DOE's efforts, two DOD programs have provided radiation portal monitors, handheld equipment, and radiation detection training to 8 countries in the former Soviet Union and Eastern Europe. Similarly, three State programs have provided radiation detection equipment and training to 31 countries since fiscal year 1994.

Regarding efforts to combat nuclear smuggling in the United States, DHS is responsible for providing radiation detection capabilities at U.S. ports of entry. Until April 2005, U.S. Customs and Border Protection (CBP) managed this program. However, on April 15, 2005, the President directed the establishment, within DHS, of the Domestic Nuclear Detection Office (DNDO), whose duties include acquiring and supporting the deployment of radiation detection equipment.[3] CBP continues its traditional screening function at ports of entry to prevent illegal immigration and interdict contraband, including the operation of radiation detection equipment. DHS is deploying portal monitors in five phases: international mail and express courier facilities; northern border crossings; major seaports; southwestern border crossings; and all other categories, including international airports and remaining border crossings, seaports, and rail crossings. Generally, CBP prioritized these categories according to their perceived vulnerability to the threat of nuclear smuggling (rather than through a formal risk assessment).

My testimony summarizes the findings of our two reports being released today on U.S. programs to combat nuclear smuggling. Specifically, I will discuss (1) the progress made by the various federal agencies tasked with installing radiation detection equipment at ports of entry in foreign countries and the challenges these agencies face and (2) DHS's efforts to install radiation detection equipment at U.S. ports of entry and challenges DHS faces in completing its program.

[2]In addition to the two reports being released today, in March 2005 we reported on DOE's Megaports Initiative. For additional information, see GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports*, GAO-05-375 (Washington, D.C.: Mar. 31, 2005). Through the end of fiscal year 2005, DOE had spent about $101 million to complete installations at four ports in Greece, the Netherlands, Sri Lanka, and the Bahamas. DOE anticipates completing an additional port in Spain in April 2006. DOE has signed agreements to begin work at ports in seven other countries (China, Honduras, Israel, Oman, the Philippines, Thailand, and the United Arab Emirates).

[3]See National Security Presidential Directive No. 43/Homeland Security Presidential Directive No. 14, Domestic Nuclear Detection (Apr. 15, 2005).

Summary

Regarding deployment of radiation detection equipment in foreign countries, DOE, DOD, and State have spent a total of about $178 million since fiscal year 1994 to provide assistance to 36 countries. For example, DOE's Second Line of Defense program has installed equipment at 83 sites, mostly in Russia, at a cost of about $130 million. However, DOE, DOD, and State face challenges that could compromise their programs' effectiveness, including (1) corruption of foreign border security officials, (2) technical limitations of some equipment at foreign sites, (3) problems with maintenance of some handheld equipment, and (4) the lack of infrastructure and harsh environmental conditions at some border sites.

- According to officials from several countries we visited, corruption is a pervasive problem within border security organizations. DOE, DOD, and State officials told us they are concerned that corrupt foreign border security personnel could compromise the effectiveness of U.S.-funded radiation detection equipment by either turning off equipment or ignoring alarms. To mitigate this threat, DOE and DOD plan to deploy communications links between individual border sites and national command centers so that alarm data can be simultaneously evaluated by multiple officials.

- Some portal monitors that State and other U.S. agencies previously installed at foreign border sites have technical limitations and can only detect gamma radiation, which makes them less effective at detecting weapons-usable nuclear material than equipment with both gamma and neutron radiation detection capabilities. Since 2002, DOE has maintained this equipment but has only upgraded equipment at one site. Until the remaining sites receive equipment with both gamma and neutron detection capabilities, they will be vulnerable to certain forms of nuclear smuggling.

- DOE has not systematically maintained handheld radiation detection equipment provided by State and other agencies. As a result, many pieces of handheld equipment, which are vital for border officials to conduct secondary inspections, may not function properly.

- Finally, many border sites are located in remote areas that often do not have access to infrastructure essential to operate radiation detection equipment and associated communication systems. Additionally, environmental conditions at some sites, such as extreme heat, can affect equipment performance. To mitigate these concerns, DOE, DOD, and State have provided generators and other equipment at remote border sites to ensure stable electricity supplies and, when appropriate, heat shields or other protection to ensure the effectiveness of radiation detection equipment.

In addition, State is the lead interagency coordinator charged with limiting overlap and duplication of effort among U.S. programs, but its ability to carry out this role has been limited by deficiencies in its strategic plan for interagency coordination and its lack of a comprehensive list of all U.S. radiation detection equipment provided to other countries.

Regarding deployment of radiation detection equipment at U.S. ports of entry, through December 2005, DHS had installed about 670 portal monitors— about 22 percent of the portal monitors DHS plans to deploy— at U.S. border crossings, seaports, and international mail and express courier facilities at a cost of about $286 million. DHS plans to deploy a total of 3,034 portal monitors by 2009 at a total cost of $1.3 billion. However, the final costs and deployment schedule are highly uncertain because of delays in releasing appropriated funds to contractors, difficulties in negotiating with seaport operators, and uncertainties in the type and cost of radiation detection equipment DHS plans to deploy. Specifically:

- DHS's cumbersome review process for providing requested information to the Congress has resulted in funds being unavailable until later in the fiscal year. This review process involves multiple approvals within DHS and the Office of Management and Budget and has held up the release of program funds, which has delayed the deployment of radiation detection equipment at U.S. ports of entry.

- Difficult negotiations with seaport operators about placement of portal monitors and screening of railcars have delayed deployments at U.S. seaports. Many seaport operators are concerned that radiation detection equipment may inhibit the flow of commerce through their ports. In addition, seaports are much larger than land border crossings, consist of multiple terminals, and may have multiple exits, which may require a greater number of portal monitors.

- DHS's $1.3 billion cost estimate for completing its domestic radiation detection program is uncertain, in part, because DHS would like to deploy advanced technology portal monitors that will likely cost significantly more than current models. However, tests have shown that these new advanced technology portal monitors are not demonstrably more effective than current models in their core function of identifying the presence of radiation. Consequently, it is not clear that the benefits of the new portal monitors would be worth the increased cost.

In addition, CBP officers have made progress in using radiation detection equipment correctly and adhering to inspection guidelines, but we identified ways to improve CBP's secondary inspection procedures. For example, when detection equipment alarms to indicate the presence of radioactivity, CBP officers are not expressly required to open containers and inspect their interiors, even though, under some circumstances, doing so can increase the chances that the source of radioactivity will be correctly located and identified. Furthermore, although radiological materials shipped into the United States are generally required to have a Nuclear Regulatory Commission (NRC) license, importers are not required to present these licenses at U.S. ports of entry, and CBP inspectors are not required to verify the authenticity of these licenses and do not have a system to do so. My GAO colleague, Mr. Greg Kutz, will be testifying on a GAO operation that was conducted to test CBP's inspection procedures and certain NRC licensing procedures.

In our report on U.S. efforts to combat nuclear smuggling in other countries, we made five recommendations. Specifically, we recommended that DOE take steps to upgrade U.S.-funded portal monitors in foreign countries that do not have both gamma and neutron detection capabilities and improve program cost estimates for anticorruption measures. Additionally, we recommended that State, working with DOE and DOD, ensure maintenance is provided for all handheld radiation detection equipment supplied by U.S. programs; strengthen its interagency coordination plan by including specific performance measures, overall cost estimates, and projected time frames for completion of U.S. efforts; and compile, maintain, and share a master list of all U.S. radiation detection assistance. Both DOE and State agreed with our recommendations. In our report on DHS's efforts to deploy radiation detection equipment at U.S. ports of entry, we made nine recommendations, including a series of actions designed to help DHS speed up the pace of portal monitor deployments, better account for schedule delays and cost uncertainties, make the most efficient use of program resources, and improve its ability to interdict illicit nuclear materials. DHS agreed with our recommendations and is taking steps to implement them.

Background

Detecting illicit trafficking in nuclear material is complicated because one of the materials of greatest concern—highly enriched uranium—has a relatively low level of radioactivity and is, therefore, among the most difficult to detect. In contrast, medical and industrial radioactive sources, which could be used to construct a dirty bomb, are highly radioactive and,

therefore, easier to detect. Although their levels of radioactivity differ, uranium and radioactive sources are similar in that they generally emit only gamma radiation, which is relatively easily shielded when encased in high-density material, such as lead. For example, we reported in March 2005 that a cargo container containing a radioactive source passed through radiation detection equipment DOE had installed at a foreign seaport without being detected because the source was surrounded by large amounts of scrap metal in the container.

Plutonium, another nuclear material of great concern, emits both gamma and neutron radiation. Although most currently fielded radiation detection equipment has the capability to detect both gamma and neutron radiation, shielding neutron radiation can be more difficult than shielding gamma radiation. Consequently, plutonium can usually be detected by a neutron detector regardless of the amount of shielding from high-density material. According to DOE officials, neutron radiation alarms are caused only by man-made materials, such as plutonium, while gamma radiation alarms are caused by a variety of naturally occurring sources, including commercial goods such as bananas, ceramic tiles, and fertilizer, as well as by dangerous nuclear materials, such as uranium and plutonium.

Because of the complexities of detecting and identifying nuclear material, customs officers and border guards who are responsible for operating detection equipment must be trained in using handheld radiation detectors to pinpoint the source of an alarm, identify false alarms, and properly respond to cases of nuclear smuggling. The manner in which radiation detection equipment is deployed, operated, and maintained can also limit its effectiveness. Given the difficulties in detecting certain nuclear materials and the inherent limitations of currently deployed radiation detection equipment, it is important that the equipment be installed, operated, and maintained in a way that optimizes authorities' ability to interdict illicit nuclear materials.

Although efforts to combat nuclear smuggling through the installation of radiation detection equipment are important, the United States should not and does not rely upon radiation detection equipment at U.S. or foreign borders as its sole means for preventing nuclear materials or a nuclear warhead from reaching the United States. Recognizing the need for a broad approach to the problem, the U.S. government has multiple initiatives that are designed to complement each other that provide a layered defense against nuclear terrorism. For example, DOE works to secure nuclear material and warheads at their sources through programs that improve the physical security at nuclear facilities in the former Soviet

Union and in other countries. In addition, DHS has other initiatives to identify containers at foreign seaports that are considered high risk for containing smuggled goods, such as nuclear and other dangerous materials. Supporting all of these programs is intelligence information that can give advanced notice of nuclear material smuggling and is a critical component to prevent dangerous materials from entering the United States.

U.S. Efforts to Provide Radiation Detection Equipment to Other Countries Face Corruption, Maintenance, and Coordination Challenges

One of the main U.S. efforts providing radiation detection equipment to foreign governments is DOE's Second Line of Defense program, which began installing equipment at key sites in Russia in 1998. According to DOE, through the end of fiscal year 2005, the program had spent about $130 million to complete installations at 83 sites, mostly in Russia. Ultimately, DOE plans to install radiation detection equipment at a total of about 350 sites in 31 countries by 2012 at a total cost of about $570 million. In addition to DOE's efforts, other U.S. agencies also have programs that provide radiation detection equipment and training to foreign governments. Two programs at DOD—the International Counterproliferation Program and Weapons of Mass Destruction Proliferation Prevention Initiative—have provided equipment and related training to eight countries in the former Soviet Union and Eastern Europe at a cost of about $22 million. Similarly, three programs at State—the Nonproliferation and Disarmament Fund, Georgia Border Security and Law Enforcement program, and Export Control and Related Border Security program—have spent about $25 million to provide radiation detection equipment and training to 31 countries.

However, these agencies face a number of challenges that could compromise their programs' effectiveness, including (1) corruption of foreign border security officials, (2) technical limitations of equipment at some foreign sites, (3) problems with maintenance of handheld equipment, and (4) the lack of infrastructure and harsh environmental conditions at some border sites. First, according to officials from several recipient countries we visited, corruption is a pervasive problem within the ranks of border security organizations. DOE, DOD, and State officials told us they are concerned that corrupt foreign border security personnel could compromise the effectiveness of U.S.-funded radiation detection equipment by either turning off equipment or ignoring alarms. To mitigate this threat, DOE and DOD plan to deploy communications links between individual border sites and national command centers so that alarm data can be simultaneously evaluated by multiple officials, thus establishing redundant layers of accountability for alarm response. In addition, DOD

plans to implement a program in Uzbekistan to combat some of the underlying issues that can lead to corruption through periodic screening of border security personnel.

Second, some radiation portal monitors that State and other U.S. agencies previously installed have technical limitations: they can detect only gamma radiation, making them less effective at detecting some nuclear material than equipment with both gamma and neutron radiation detection capabilities. Through an interagency agreement, DOE assumed responsibility for ensuring the long-term sustainability and continued operation of radiation portal monitors and X-ray vans equipped with radiation detectors that State and other U.S. agencies provided to 23 countries. Through this agreement, DOE provides spare parts, preventative maintenance, and repairs for the equipment through regularly scheduled maintenance visits. Since 2002, DOE has maintained this equipment but has not upgraded any of it, with the exception of at one site in Azerbaijan. According to DOE officials, new implementing agreements with the appropriate ministries or agencies within the governments of each of the countries where the old equipment is located are needed before DOE can install more sophisticated equipment.

Third, since 2002, DOE has been responsible for maintaining certain radiation detection equipment previously deployed by State and other agencies in 23 countries. However, DOE is not responsible for maintaining handheld radiation detection equipment provided by these agencies. As a result, many pieces of handheld equipment, which are vital for border officials to conduct secondary inspections of vehicles or pedestrians, may not function properly. For example, in Georgia, we observed border guards performing secondary inspections with a handheld radiation detector that had not been calibrated (adjusted to conform with measurement standards) since 1997. According to the detector's manufacturer, yearly recalibration is necessary to ensure that the detector functions properly.

Finally, many border sites are located in remote areas that often do not have access to reliable supplies of electricity, fiber optic lines, and other infrastructure essential to operate radiation detection equipment and associated communication systems. Additionally, environmental conditions at some sites, such as extreme heat, can affect the performance of equipment. To mitigate these concerns, DOE, DOD, and State have provided generators and other equipment at remote border sites to ensure stable supplies of electricity and, when appropriate, heat shields or other protection to ensure the effectiveness of radiation detection equipment.

We also reported that State's ability to carry out its role as lead interagency coordinator of U.S. radiation detection equipment assistance has been limited by deficiencies in its strategic plan for interagency coordination and by its lack of a comprehensive list of all U.S. radiation detection equipment assistance. In response to a recommendation we made in 2002, State led the development of a governmentwide plan to coordinate U.S. radiation detection equipment assistance overseas. This plan broadly defines a set of interagency goals and outlines the roles and responsibilities of participating agencies. However, the plan lacks key components, including overall program cost estimates, projected time frames for program completion, and specific performance measures. Without these elements in the plan, State will be limited in its ability to effectively measure U.S. programs' progress toward achieving the interagency goals.

Additionally, in its role as lead interagency coordinator, State has not maintained accurate information on the operational status and location of all radiation detection equipment provided by U.S. programs. While DOE, DOD, and State each maintain lists of radiation detection equipment provided by their programs, they do not regularly share such information, and no comprehensive list of all equipment provided by U.S. programs exists. For example, according to information we received from program managers at DOE, DOD, and State, more than 7,000 pieces of handheld radiation detection equipment had been provided to 36 foreign countries through the end of fiscal year 2005. Because much of this equipment was provided to the same countries by multiple agencies and programs, it is difficult to determine the degree to which duplication of effort has occurred. Without a coordinated master list of all U.S.-funded equipment, program managers at DOE, DOD, and State cannot accurately assess if equipment is operational and being used as intended, determine the equipment needs of countries where they plan to provide assistance, or detect whether an agency has unknowingly supplied duplicative equipment.

DHS Has Made Progress in Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain

Through December 2005, DHS had installed about 670 radiation portal monitors nationwide— about 22 percent of the portal monitors DHS plans to deploy—at international mail and express courier facilities, land border crossings, and seaports in the United States. DHS has completed portal monitor deployments at international mail and express courier facilities and the first phase of northern border sites—57 and 217 portal monitors, respectively. In addition, by December 2005, DHS had deployed 143 of 495 portal monitors at seaports and 244 of 360 at southern border sites.[4] As of February 2006, CBP estimated that, with these deployments, it has the ability to screen about 62 percent of all containerized shipments entering the United States (but only 32 percent of all containerized seaborne shipments) and roughly 77 percent of all private vehicles. DHS plans to deploy 3,034 portal monitors by September 2009 at a cost of $1.3 billion. However, the final costs and deployment schedule are highly uncertain because of delays in releasing appropriated funds to contractors, difficulties in negotiating with seaport operators, and uncertainties in the type and cost of radiation detection equipment DHS plans to deploy. Further, to meet this goal, DHS would have to deploy about 52 portal monitors a month for the next 4 years—a rate that far exceeds the 2005 rate of about 22 per month.

In particular, several factors have contributed to the delay in the deployment schedule. First, DHS provides the Congress with information on portal monitor acquisitions and deployments before releasing any funds. However, DHS's cumbersome review process has consistently caused delays in providing such information to the Congress. For example, according to the House Appropriations Committee report on DHS's fiscal year 2005 budget, CBP should provide the Congress with an acquisition and deployment plan for the portal monitor program prior to funding its contractors. This plan took many months to finalize, mostly because it required multiple approvals within DHS and the Office of Management and Budget prior to being submitted to the Congress. The lengthy review process delayed the release of funds and, in some cases, disrupted and delayed deployment.

Second, difficult negotiations with seaport operators about placement of portal monitors and screening of railcars have delayed deployments at U.S. seaports. Many seaport operators are concerned that radiation

[4]In addition, three portal monitors had been installed at the Nevada Test Site to analyze their detection capabilities, and four had been retrofitted at express mail facilities.

detection equipment may inhibit the flow of commerce through their ports. In addition, seaports are much larger than land border crossings, consist of multiple terminals, and may have multiple exits, which may require a greater number of portal monitors. Further, devising an effective way to conduct secondary inspections of rail traffic as it departs seaports without disrupting commerce has delayed deployments. This problem may worsen because the Department of Transportation has forecast that the use of rail transit out of seaports will probably increase in the near future.

Finally, DHS's $1.3 billion estimate for the project is highly uncertain, in part, because of uncertainties in the type and cost of radiation detection equipment that DHS plans to deploy. The estimate is based on DHS's plans for widespread deployment of advanced technology portal monitors, which are currently being developed. However, the prototypes of this equipment have not yet been shown to be more effective than the portal monitors now in use, and DHS officials say they will not purchase the advanced portal monitors unless they are proven to be clearly superior. Moreover, when advanced technology portal monitors become commercially available, experts estimate that they will cost between about $330,000 and $460,000 each, far more than the currently used portal monitors whose costs range from about $49,000 to $60,000. Even if future test results indicate better detection capabilities, without a detailed comparison of the two technologies' capabilities it would not be clear that the dramatically higher cost for this new equipment would be worth the investment.

We also identified potential issues with the procedures CBP inspectors use to perform secondary inspections that, if addressed, could strengthen the nation's defenses against nuclear smuggling. For example, CBP's procedures require only that officers locate, isolate, and identify radiological material. Typically, officers perform an external examination by scanning the sides of cargo containers with handheld radiation detection equipment during secondary inspections. CBP's guidance does not specifically require officers to open containers and inspect their interiors, even when their external examination cannot unambiguously resolve the alarm. However, under some circumstances, opening containers can improve security by increasing the chances that the source of radioactivity that originally set off the alarm will be correctly located and identified. The second potential issue with CBP's procedures involves NRC documentation. Individuals and organizations shipping radiological materials to the United States must generally acquire a NRC license, but according to NRC officials, the license does not have to accompany the shipment. Although inspectors examine such licenses when these

shipments arrive at U.S. ports of entry, CBP officers are not required to verify that shippers of radiological material actually obtained required licenses and to authenticate licenses that accompany shipments. We found that CBP inspectors lack access to NRC license data that could be used to authenticate a license at the border.

This concludes my prepared statement. I would be happy to respond to any questions that you or other Members of the Subcommittee may have.

GAO Contact and Staff Acknowledgments

For further information about this testimony, please contact me at (202) 512-3841 or at aloisee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. R. Stockton Butler, Nancy Crothers, Jim Shafer, and Eugene Wisnoski made key contributions to this statement.

Related GAO Products

Combating Nuclear Smuggling: DHS Has Made Progress in Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain. GAO-06-389. Washington, D.C.: March 22, 2006.

Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries. GAO-06-311. Washington, D.C.: March 14, 2006.

Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and in Other Countries. GAO-05-840T. Washington, D.C.: June 21, 2005.

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. GAO-05-375. Washington, D.C.: March 31, 2005.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. GAO-03-297T. Washington, D.C.: November 18, 2002.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling. GAO-02-989T Washington, D.C.: July 30, 2002.

Nuclear Nonproliferation: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning. GAO-02-426. Washington, D.C.: May 16, 2002.

*

United States Government Accountability Office

GAO

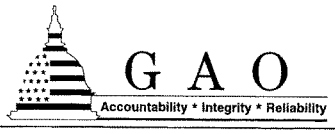
Testimony
Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate

For Release on Delivery
Expected at 9:30 a.m. EST
Tuesday, March 28, 2006

BORDER SECURITY

Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations



GAO-06-583T

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss our investigation of potential security weaknesses associated with the installation of radiation detection equipment at U.S. ports of entry. To address the threat of dirty bombs and other nuclear material, the federal government has programs in place that regulate the transportation of radioactive sources and to prevent illegal transport of radioactive sources across our nation's borders. The Department of Homeland Security through the U.S. Customs and Border Protection (CBP) uses radiation detection equipment at ports of entry to prevent such illicit entry of radioactive sources. The goal of CBP's inspection program is to "...thwart the operations of terrorist organizations by detecting, disrupting, and preventing the cross-border travel of terrorists, terrorist funding, and terrorist implements, including Weapons of Mass Destruction and their precursors." Deploying radiation detection equipment is part of CBP's strategy for thwarting radiological terrorism and CBP is using a range of such equipment to meet its goal of screening all cargo, vehicles, and individuals coming into the United States.

Most travelers enter the United States through the nation's 154 land border ports of entry. CBP inspectors at ports of entry are responsible for the primary inspection of travelers to determine their admissibility into the United States and to enforce laws related to preventing the entry of contraband, such as drugs and weapons of mass destruction.

Our investigation was conducted at your request as a result of widespread congressional and public interest in the security of our nation's borders, given today's unprecedented terrorism threat environment. Our investigation was conducted under the premise that given today's security environment, our nation's borders must be protected from the smuggling of radioactive sources by terrorists.

This testimony will provide the results of our work related to testing whether the radiation portal monitors installed at the U.S. ports of entry would detect radioactive sources transported in vehicles attempting to enter the United States. We will also provide our observations regarding the procedures that CBP inspectors followed when the radiation portal monitors detected such material. We are releasing a detailed report today with corrective action briefings to CBP and the Nuclear Regulatory

Commission (NRC) on the results of our undercover border crossing tests.[1]

We selected two land ports of entry that had radiation portal monitors installed: one at the U.S.-Canadian border and one at the U.S.-Mexican border. Radiation portal monitors are large pieces of stationary equipment that CBP uses as part of its overall strategy to thwart radiological terrorism by detecting the presence of radioactive sources by screening people, vehicles, and cargo as they pass through ports of entry. In order to safely plan and execute our undercover operation, several of our investigators attended training at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland. Our investigators received training on the safe handling, storage, and transport of radioactive sources.

When considering the type of radioactive sources to use in our undercover operation, we decided to use one of the most common radioisotopes used in industry for its strong radioactivity and also used in medical therapy to treat cancer. When considering the amount of radioactive sources to use in our undercover operation, we decided to use an amount NIST officials determined is sufficient to manufacture a dirty bomb[2] for two simultaneous border crossings. A dirty bomb would most likely result in small radiation exposures and would typically not contain enough radiation to kill people or cause severe illnesses. However, by scattering the radioactive material, the dirty bomb has the effect of contaminating an area. The extent of local contamination depends on several factors, including the size of the explosive, the amount and type of radioactive material used, and weather conditions. While there could be an increase in the cancer risk among those exposed to radiation from a dirty bomb, the more significant effect of a dirty bomb could be the closing of contaminated areas. The direct costs of cleanup and the indirect losses in trade and business in the contaminated areas could be large. Hence, dirty

[1]GAO, *Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation's Borders at Selected Locations*, GAO-06-545R (Washington, D.C.: Mar. 28, 2006).

[2]According to the Centers for Disease Control and Prevention, a dirty bomb is a mix of explosives, such as dynamite, with radioactive powder or pellets. When the dynamite or other explosives are set off, the blast carries radioactive material into the surrounding area.

bombs are generally considered to be weapons of mass disruption instead of weapons of mass destruction.

As part of our investigation, we purchased a small quantity of the radioactive sources from a commercial source by posing as an employee of a fictitious company. This was to demonstrate that anyone can purchase small quantities of radioactive sources for stockpiling because suppliers are not required to exercise due diligence to determine whether the buyer has a legitimate use for the radioactive sources and suppliers are not required to ask the buyer to produce an NRC document when making purchases in small quantities. We then deployed two teams of investigators to the field to make simultaneous border crossings at the northern and southern borders in an attempt to transport radioactive sources into the United States.

While making our simultaneous crossings, we focused our investigation on whether the radiation portal monitors would detect the radioactive sources we carried and whether CBP inspectors exercised due diligence to determine the authenticity of paperwork presented by individuals attempting to transport radioactive sources across our borders. Although we offer observations on the procedures that CBP inspectors followed for our two border crossings, we did not evaluate the adequacy of the design or effectiveness of those procedures. Our investigation also tested whether an NRC document could be counterfeited using data easily accessible and available to the public. We conducted our investigation from July 2005 through December 2005 in accordance with quality standards for investigations as set forth by the President's Council on Integrity and Efficiency.

Summary

For the purposes of this undercover investigation, we purchased a small amount of radioactive sources and one container used to store and transport the material from a commercial source over the telephone. One of our investigators, posing as an employee of a fictitious company located in Washington, D.C., stated that the purpose of his purchase was to use the radioactive sources to calibrate personal radiation detection pagers. The purchase was not challenged because suppliers are not required to determine whether a buyer has a legitimate use for the radioactive sources, nor are suppliers required to ask the buyer to produce an NRC document when making purchases in small quantities.

The radiation portal monitors properly signaled the presence of radioactive material when our two teams of investigators conducted simultaneous border crossings. Our investigators' vehicles were inspected

in accordance with most of the CBP policy at both the northern and southern borders. However, our investigators were able to enter the United States with enough radioactive sources to make two dirty bombs using counterfeit documents. Specifically, they were able to successfully represent themselves as employees of a fictitious company and present a counterfeit bill of lading and a counterfeit NRC document during the secondary inspections at both locations. The CBP inspectors never questioned the authenticity of the investigators' counterfeit bill of lading or the counterfeit NRC document authorizing them to receive, acquire, possess, and transfer radioactive sources.

Documentation Was Produced to Support Undercover Investigation

As part of our undercover investigation, we produced counterfeit documents before sending our two teams of investigators out to the field. We found two NRC documents and a few examples of the documents by searching the Internet.[3] We subsequently used commercial, off-the-shelf computer software to produce two counterfeit NRC documents authorizing the individual to receive, acquire, possess, and transfer radioactive sources.

To support our investigators' purported reason for having radioactive sources in their possession when making their simultaneous border crossings, a GAO graphic artist designed a logo for our fictitious company and produced a bill of lading using computer software.

With Ease, Investigators Purchased, Received, and Transported Radioactive Sources Across Both Borders

Our two teams of investigators each transported an amount of radioactive sources sufficient to manufacture a dirty bomb when making their recent, simultaneous border crossings. In support of our earlier work, we had obtained an NRC document and had purchased radioactive sources as well as two containers to store and transport the material.

For the purposes of our current undercover investigation, we purchased a small amount of radioactive sources and one container for storing and transporting the material from a commercial source over the telephone. One of our investigators, posing as an employee of a fictitious company, stated that the purpose of his purchase was to use the radioactive sources to calibrate personal radiation detectors. Suppliers are not required to exercise any due diligence in determining whether the buyer has a legitimate use for the radioactive sources, nor are suppliers required to ask the buyer to produce an NRC document when making purchases in small

[3]None of these documents were available on NRC's Web site.

quantities. The amount of radioactive sources our investigator sought to purchase did not require an NRC document. The company mailed the radioactive sources to an address in Washington, D.C.

Two Teams of Investigators Conducted Simultaneous Crossings at the U.S.-Canadian Border and U.S.-Mexican Border

Northern Border Crossing

On December 14, 2005, our investigators placed two containers of radioactive sources into the trunk of their rental vehicle. Our investigators – acting in an undercover capacity – drove to an official port of entry between Canada and the United States. They also had in their possession a counterfeit bill of lading in the name of a fictitious company and a counterfeit NRC document.

At the primary checkpoint, our investigators were signaled to drive through the radiation portal monitors and to meet the CBP inspector at the booth for their primary inspection. As our investigators drove past the radiation portal monitors and approached the primary checkpoint booth, they observed the CBP inspector look down and reach to his right side of his booth. Our investigators assumed that the radiation portal monitors had activated and signaled the presence of radioactive sources. The CBP inspector asked our investigators for identification and asked them where they lived. One of our investigators on the two-man undercover team handed the CBP inspector both of their passports and told him that he lived in Maryland while the second investigator told the CBP inspector that he lived in Virginia.

The CBP inspector also asked our investigators to identify what they were transporting in their vehicle. One of our investigators told the CBP inspector that they were transporting specialized equipment back to the United States. A second CBP inspector, who had come over to assist the first inspector, asked what else our investigators were transporting. One of

our investigators told the CBP inspectors that they were transporting radioactive sources for the specialized equipment. The CBP inspector in the primary checkpoint booth appeared to be writing down the information. Our investigators were then directed to park in a secondary inspection zone, while the CBP inspector conducted further inspections of the vehicle.

During the secondary inspection, our investigators told the CBP inspector that they had an NRC document and a bill of lading for the radioactive sources. The CBP inspector asked if he could make copies of our investigators' counterfeit bill of lading on letterhead stationery as well as their counterfeit NRC document. Although the CBP inspector took the documents to the copier, our investigators did not observe him retrieving any copies from the copier.

Our investigators watched the CBP inspector use a handheld Radiation Isotope Identifier Device (RIID), which he said is used to identify the source of radioactive sources, to examine the investigators' vehicle. He told our investigators that he had to perform additional inspections. After determining that the investigators were not transporting additional sources of radiation, the CBP inspector made copies of our investigators' drivers' licenses, returned their drivers' licenses to them, and our investigators were then allowed to enter the United States. At no time did the CBP inspector question the validity of the counterfeit bill of lading or the counterfeit NRC document.

Southern Border Crossing

On December 14, 2005, our investigators placed two containers of radioactive sources into the trunk of their vehicle. Our investigators drove to an official port of entry at the southern border. They also had in their possession a counterfeit bill of lading in the name of a fictitious company and a counterfeit NRC document.

At the primary checkpoint, our two-person undercover team was signaled by means of a traffic light signal to drive through the radiation portal monitors and stopped at the primary checkpoint for their primary inspection. As our investigators drove past the portal monitors and approached the primary checkpoint, they observed that the CBP inspector remained in the primary checkpoint for several moments prior to approaching our investigators' vehicle. Our investigators assumed that the radiation portal monitors had activated and signaled the presence of radioactive sources.

The CBP inspector asked our investigators for identification and asked them if they were American citizens. Our investigators told the CBP inspector that they were both American citizens and handed him their state-issued drivers' licenses. The CBP inspector also asked our investigators about the purpose of their trip to Mexico and asked whether they were bringing anything into the United States from Mexico. Our investigators told the CBP inspector that they were returning from a business trip in Mexico and were not bringing anything into the United States from Mexico.

While our investigators remained inside their vehicle, the CBP inspector used what appeared to be a RIID to scan the outside of the vehicle. One of our investigators told him that they were transporting specialized equipment. The CBP inspector asked one of our investigators to open the trunk of the rental vehicle and to show him the specialized equipment. Our investigator told the CBP inspector that they were transporting radioactive sources in addition to the specialized equipment. The primary CBP inspector then directed our investigators to park in a secondary inspection zone for further inspection.

During the secondary inspection, the CBP inspector said he needed to verify the type of material our investigators were transporting, and another CBP inspector approached with what appeared to be a RIID to scan the cardboard boxes where the radioactive sources was placed. The instrumentation confirmed the presence of radioactive sources.

When asked again about the purpose of their visit to Mexico, one of our investigators told the CBP inspector that they had used the radioactive sources in a demonstration designed to secure additional business for their company. The CBP inspector asked for paperwork authorizing them to transport the equipment to Mexico. One of our investigators provided the counterfeit bill of lading on letterhead stationery, as well as their counterfeit NRC document. The CBP inspector took the paperwork provided by our investigators and walked into the CBP station. He returned several minutes later and returned the paperwork. At no time did the CBP inspector question the validity of the counterfeit bill of lading or the counterfeit NRC document.

Corrective Action Briefings

We conducted corrective action briefings with CBP and NRC officials shortly after completing our undercover operations. On December 21, 2005, we briefed CBP officials about the results of our border crossing tests. CBP officials agreed to work with the NRC and CBP's Laboratories

and Scientific Services to come up with a way to verify the authenticity of NRC materials documents.

We conducted two corrective action briefings with NRC officials on January 12 and January 24, 2006, about the results of our border crossing tests. NRC officials disagreed with the "concern threshold" that NIST officials provided to us concerning the amount of radioactive sources needed to produce a dirty bomb, noting that NRC's "concern threshold" is significantly higher than NIST's. We continue to believe that our purchase of radioactive sources and our ability to counterfeit an NRC document are matters that NRC should address. We could have purchased all of the radioactive sources used in our two undercover border crossings by making multiple purchases from different suppliers, using similarly convincing cover stories, using false identities, and had all of the radioactive sources conveniently shipped to our nation's capital.

Further, we believe that the amount of radioactive sources that we were able to transport into the United States during our operation would be sufficient to produce two dirty bombs, which could be used as weapons of mass disruption. Finally, NRC officials told us that they are aware of the potential problems of counterfeiting documents and that they are working to resolve these issues.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you or other members of the committee may have at this time.

Contacts and Acknowledgments

For further information about this testimony, please contact Gregory D. Kutz at (202) 512-7455 or kutzg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony.

Testimony of David Huizenga
Assistant Deputy Administrator
Office of International Material Protection and Cooperation
Defense Nuclear Nonproliferation
National Nuclear Security Administration
to the
U.S. Senate Committee on Homeland Security and Governmental Affairs
Permanent Subcommittee on Investigations
March 28, 2006

Thank you Mr. Chairman, Ranking Member Levin and other distinguished members of the Subcommittee. I am pleased to appear before you today to share the progress we have made under the Second Line of Defense (SLD) program to deploy radiation detection equipment at strategic international locations.

I am the Assistant Deputy Administrator for the National Nuclear Security Administration's (NNSA) Office of International Material Protection and Cooperation (IMPC). My office is one of six program offices within the Office of Defense Nuclear Nonproliferation (DNN). The collective mission of DNN is to detect, prevent, and reverse the proliferation of weapons of mass destruction. Our programs are structured in support of multiple layers of defense against nuclear terrorism and state-sponsored nuclear proliferation. This multi-layered approach is intended to identify and address potential vulnerabilities within the international nonproliferation regime, to limit terrorists' access to deadly weapons and material, and to prevent the illicit trafficking of dangerous materials that could be used in a nuclear or radiological weapon.

For the last decade and a half we have focused on securing nuclear materials and weapons at well over one hundred research, storage and manufacturing facilities in Russia and other states of the Former Soviet Union. Our longstanding nonproliferation programs in international safeguards and export controls have existed for more than thirty years, but the dramatic increase in our efforts to secure nuclear material took place in the years following the demise of the Soviet Union. This focus on securing nuclear weapons and materials is the first line of defense in our strategy to deny

terrorists access to the essential element of a nuclear weapon, fissile material. We are scheduled to complete nuclear security upgrades at all facilities by the end of 2008. The Second Line of Defense Program is a natural complement to these activities and supports the multi-layered defense system to protect the U.S. homeland from attack by a nuclear or radiological dispersal device. All of our efforts are centered on the premise that confronting the threat of nuclear terrorism as close to the source of the threat as possible, far from our borders, is the most effective means to reduce the risk of an attack.

I'd like to make a few points on the nuclear smuggling threat. As the director of several US programs to secure nuclear materials abroad, I have some insight into the threat of material diversion from nuclear facilities - the first step in the nuclear smuggling chain.

Our security assistance programs abroad dramatically reduce the risk of nuclear material theft. However, every security system ultimately depends on the people operating it - the so-called "human factor". Motivated by greed, coercion, or debt, facility insiders may successfully divert nuclear materials. This problem is compounded by the large number of nuclear facilities out there - each presenting a unique opportunity for material diversion. Established crime groups are operating on the periphery of many of these facilities. These groups are often engaged in smuggling a variety of goods. If a single nuclear smuggling network materializes and operates successfully, even for a short period, a "goal quantity" of nuclear material may reach our enemies. There is only one way to combat a threat this diverse and complex - a redundant and layered defense. I can't emphasize enough how important this is. If human error or corruption enables smugglers to bypass one layer, our only hope is to catch them at the next.

While the body of verified nuclear smuggling cases is studied intensely inside and outside government, we must continuously remind ourselves of how much we don't know. We don't know how many networks have operated successfully, or how many are operating now. As stewards of U.S. national security in this regard, we have to assume there are groups colluding to smuggle these materials today - and aggressively pursue every opportunity to disrupt them, before they become nuclear material "pipelines" to our enemies. The consequences of failure are just too great to do otherwise.

The Second Line of Defense Program accomplishes its goals to deter, detect, and interdict illicit trafficking of nuclear and radiological material across international borders by partnering with host countries throughout the world. We provide detection equipment, training, and system maintenance and repair support to the host country. The Program closely coordinates these international efforts with other U.S. Government Agencies such as the Departments of State, Defense, and Homeland Security.

The SLD Program has two main components: the Core Program and the Megaports Initiative. The Core Program plans to deploy radiation detection systems at approximately 350 land border crossings, airports, and feeder ports in Russia and other countries of the former Soviet States, Eastern Europe, the Mediterranean region and other key countries. Under our Megaports Initiative, NNSA plans to equip approximately 70 major international seaports with radiation detection equipment to scan cargo containers for nuclear and other radiological materials.

PROGRESS IN SLD CORE PROGRAM

The SLD Core program has been working cooperatively with the Federal Customs Service of the Russian Federation since 1998, to secure Russian points of entry and exit against the nuclear smuggling threat. Of the estimated 350 international points of entry in the Russian Federation, NNSA has provided radiation detection systems at 78 of the 120 planned border crossings, airports and seaports. Our Russian Customs partners have installed monitors at approximately 120 additional sites and will fund installations at the remaining 110 sites.

But installation of systems alone does not fully address the challenge of nuclear smuggling. If the systems are not maintained and if personnel are not properly trained to use them, our efforts are largely in vain. In April of 2005 NNSA and Russian Customs signed an agreement to document our mutual commitment to ensuring the long term maintenance and sustainability of the radiation detection systems deployed in Russia. The agreement primarily provides for the training of Russian Customs officials and periodic maintenance of equipment. NNSA and Russian Customs have demonstrated our commitment to this issue with the recent award of two contracts, one by NNSA and one by Russian Customs, to provide for the repair, periodic maintenance and calibration of all equipment that is currently installed. In the area of training, the SLD Program has worked

closely with Russian Customs over the past several years to develop and institutionalize within the Customs Academies a comprehensive training program, to include development of curricula, text books, training materials and simulators, which have been used to train over 500 Customs nuclear and radiological material specialists. In addition, over 1,000 first line responders (i.e., the officials who actually respond to the alarm and detain the vehicle or person) have also been trained. In 2005, SLD supported and observed a Russian interagency interdiction exercise held in Vladivostok to evaluate the ability of trained FCS personnel to successfully respond to illicit trafficking of nuclear and radioactive materials passing through a Customs site and to test the Russian interagency response system. We were pleased to see an effective system in operation.

Our cooperative work in Russia remains one of our top priorities, but we realize that deployment of radiation detection systems and the training and technical support necessary to effectively operate them is needed not just in Russia, but also along potential smuggling pathways in additional countries. Since the data set on nuclear smuggling is limited, it cannot be the sole source for determinations of trends and tactics in SNM smuggling. Therefore our prioritization activities also consider data from government and outside sources, commissioned studies, discussions with host countries, and SLD developed computer modeling. As a result of this comprehensive analysis, SLD separated countries of interest into four prioritized groups with Russia remaining our highest priority.

As a result of these our prioritization efforts, and in coordination with the Departments of State and other agencies, we have expanded the SLD program beyond Russia and are now actively installing or have installed equipment in other countries throughout the FSU and Eastern Europe, including Ukraine, Georgia, Azerbaijan, Kyrgyzstan, Slovenia, Greece and Lithuania. In total, we have identified approximately 230 sites in 29 countries outside of Russia where we believe that the installation of radiation detection systems should reduce the risk of nuclear smuggling. Based on current planning, we anticipate that we will complete installations at 225 sites within the countries in the two highest priority groups by the end of FY 2009, with the remaining installations completed by the end of FY 2013.

MAINTENANCE PROGRAM

In 2002, in accordance with the recommendation of the Government Accountability Office, the NNSA assumed responsibility for maintaining radiation detection equipment, and x-ray vans provided by other US government agencies between 1992-2002 in 23 former Soviet Republics and Central European countries. In addition to providing maintenance and repair services for the monitors and x-ray vans, the SLD program also provides maintenance support for the handheld detection equipment distributed to support the fixed portal monitors. Of these 23 countries, eleven received radiation detection portal monitors and the remainder received x-ray vans. The monitors deployed by these other agencies are of the single channel variety that can only detect gamma radiation, reducing their effectiveness against some types of materials of concern. We are in the process of upgrading these portal monitors with more effective dual-channel equipment. In many instances, we will replace this equipment as part of the implementation of the comprehensive SLD program in the country. We plan in to complete upgrades of the monitors by the end of 2007. In accordance with the Government Accountability Office's 2002 recommendation to consolidate maintenance activities within DOE, the SLD program will additionally assume responsibility for the maintenance and sustainability of the radiation detection equipment deployed in Uzbekistan by Department of Defense and Armenia by the Department of State.

GAO REPORT

Now that I have given you a brief background of the NNSA/SLD Core Program and its technical capabilities and interagency relationships, I would like to address some issues about the program raised by the Government Accountability Office (GAO). The recent GAO report entitled "Combating Nuclear Smuggling" addressed the Core Program and pointed out two main areas of concern. One is combating corruption from within the countries where we deploy nuclear detection equipment and the other is the replacement and upgrade of the older equipment previously installed by others. The SLD Program is specifically structured to address both of these issues.

With regard to the potential corruption of host country operators, we seek to address this challenge by ensuring that all radiation portal monitors deployed under comprehensive SLD installations be networked to at least one central alarm station. The associated communications software requires reporting by a host country operator on the cause of an alarm and a summary of the actions taken in response to the alarm. Installations and operations are structured so that more than one person will be involved in reviewing and closing an alarm, thus making it more difficult for a corrupt official to bypass the system. Additionally, to protect against corruption at a single site, the SLD strategy calls for the placement of monitors on both sides of the border at certain high priority locations resulting in redundant layers of detection in different countries. We are also developing the means to send status of health, alarm and other data to central locations within the host country for further in-depth review and technical assistance. Such a system is being deployed in Greece and will soon be available in Russia. Based on these experiences, the Program plans to deploy these systems more widely taking into account country specific factors, such as communications infrastructure and host nation capabilities.

As to upgrading the less sophisticated portal monitors previously installed by other US agencies, as I stated previously, by the end of FY 2007, NNSA intends to replace all single monitors with dual channel equipment as part of our comprehensive SLD Core strategy. Upgraded handheld detection equipment for secondary inspections will also be provided. The majority of these older monitors are currently being replaced as part of the comprehensive country-wide installations underway in Ukraine, Slovenia, Georgia and Azerbaijan. In lower priority countries, where SLD is not scheduled to work for several years, monitors will be replaced if they are in active locations and being put to effective use by the host countries. Broader communication systems and training will be provided later when we engage in comprehensive country-wide activities.

Accelerating the Megaports Initiative

In order to complement our security efforts in U.S. ports we established the Megaports Initiative in 2003 to provide early detection of possible illicit trafficking of nuclear materials before they enter our territory. Under the Megaports program, NNSA installs radiation detection systems at foreign ports to enhance the detection and interdiction capabilities of the customs

authorities within our partner countries. The program is designed to provide the capacity to screen import, export and as much transshipped containerized cargo as possible, while posing minimal impact on seaport operations. This initiative provides an added layer of defense against the threat of dangerous material reaching our shores, but does not eliminate the crucial role played by U.S. Customs officials, both in foreign ports and here at home.

The primary mission of the Megaports program is to prevent terrorists from successfully moving these dangerous materials through a major foreign port facility for use in an attack against the United States or our partners. In recognition of the fact that in today's globalized economy a nuclear or radiological incident at one port could adversely impact nearly every major economy, the Megaports program serves to enhance the security of the global maritime shipping system and protect global economic stability.

I would like to take a few minutes to provide you with an update on our progress in the implementation of this important initiative. We have made steady progress in implementing this international port security program since the inception of the Megaports Initiative in 2003. We have identified approximately 70 ports of interest in 35 countries based on the volume of containers coming to the U.S. from these ports and also considering regional threat. The Megaports program is currently operational in Greece, the Bahamas, Sri Lanka and the Netherlands and will be fully operational in Spain in the Spring of 2006. We are at various stages of design and construction in nine additional countries: Belgium, China, the U.A.E., Honduras, Israel, Oman, the Philippines, Singapore and Thailand. Finally, we are aggressively pursuing agreements with many of the remaining 21 countries of interest.

As an integral element of the U.S. maritime security strategy, the Megaports Initiative complements the efforts of the Department of Homeland Security's (DHS) Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), Coast Guard's International Port Security Program (IPSP) and the Department of State's Proliferation Security Initiative (PSI). We work in lock-step with the Department of Homeland Security's Bureau of Customs and Border Protection's (CBP) CSI program to ensure that our efforts are coordinated in those ports in which we are both working. We have signed a memorandum of understanding with CBP and have committed to install radiation detection equipment at all CSI ports. As our common goal is to prevent WMD from reaching U.S. ports, the

Megaports initiative reinforces CBP's targeting, screening and scanning processes by providing additional scanning capability for radioactive materials.

We will continue to work closely with our CBP and Domestic Nuclear Detection Office (DNDO) partners to identify opportunities to accelerate the implementation of the Megaports program. We share a common vision and work to ensure that our efforts fit cohesively together in support of a comprehensive global architecture.

Detection Equipment

The radiation detection equipment currently being deployed by NNSA under the SLD program is proven technology that was developed to ensure nuclear material security at DOE weapons sites. NNSA currently provides host country partners with an integrated suite of equipment, which includes radiation portal monitors that utilize plastic scintillators and Helium-3 tube technology to detect highly enriched uranium, plutonium, and other radioactive isotopes; computer and camera equipment to collect and transmit alarm information for analysis by host country Customs officials; and handheld equipment that can be used to conduct secondary inspections to isolate and identify radioactive sources within containers, vehicles, or on persons. The equipment that we deploy has been evaluated by our technical experts at the National Laboratories as well as at the Domestic Nuclear Defense Office's test facility in Nevada and has proven to be operationally effective and robust in harsh, and often remote, international environments.

Advancements in Detection Capabilities

That being said, we all recognize that there are limitations in its capabilities and that there is a need for next generation equipment that will identify both highly enriched uranium and plutonium with a high degree of efficiency and will also identify other radioactive isotopes that are either innocent or of lesser concern. We are closely tracking the efforts within the NNSA and DNDO research and development programs so that we may capitalize on advancements in detection capabilities. For example, we are working with DNDO to purchase a number of Advanced Spectroscopic Portals (ASP) as soon as the equipment has been sufficiently evaluated and is ready for deployment. The ASP is expected to enhance the ability of Customs officials to resolve alarms by providing a more sophisticated capability to

quickly identify the radioactive isotopes of concern. NNSA plans to use the ASPs at Megaports locations as secondary inspection tools as well as at rail border crossings when infrastructure and environment permit.

We have also initiated efforts to modify existing technologies to address transshipment scanning challenges in ports. For example, in the Port of Freeport in The Bahamas, we expect to be able to scan about 90 percent of the transshipped cargo using a straddle carrier vehicle outfitted with radiation detection equipment, including spectroscopic detection capabilities. This modified straddler can travel through rows of shipping containers in the stacks, a reverse of our normal deployment strategy based on permanent placement of the detection equipment and transit of the container through the portal. While this approach is not applicable at all ports, for those terminals that stack in a compatible configuration, this type of deployment provides an opportunity to maximize screening of transshipped containers. We are also considering other mobile configurations being developed by the private sector to address similar issues at other ports.

Finally, we continue to look to the future and eagerly await the development of even more revolutionary detection enhancements, such as the Cargo Advanced Automated Radiography System (CAARS) currently under development within DNDO. This advanced radiography system will provide better imaging in drive through capacities and is expected to improve our ability to identify shielded highly enriched uranium in containerized cargo.

Integrated Cargo Inspection

For the last two years we have worked closely with DHS/CBP to evaluate the effectiveness of the Integrated Container Inspection System (ICIS), which is being piloted in the Port of Hong Kong. We have closely observed its operation and held technical discussions regarding the system with the manufacturer's representatives both in Hong Kong and at their facilities in the U.S. and remain in close communication with the terminal operators. We are fully supportive of the private sector's willingness to take the initiative to enhance the security of the international maritime trade lanes and believe that private sector container screening is compatible with our Megaports mission.

Systems with capabilities being incorporated into the ICIS pilot would provide an x-ray or gamma-ray image that supplements radiation detection alarm profiles and would provide an additional piece of information to support evaluation and dispensation of radiation alarms. We are currently working with technical experts from DHS to analyze data from the ICIS system to gain a better understanding of the system's cost-benefit factor and how effectively the integration of these technologies may improve our ability to identify shielded highly enriched uranium and to dispense innocent alarms more quickly. If terminal operators decide to deploy systems like ICIS, which integrate radiation detection, visual imaging, and optical character recognition, we believe that the data collected for those containers that trigger radiation alarms could be extracted and analyzed before the container departs the port. In support of such efforts and the Megaports program, we are prepared to provide a combination of hardware and technical assistance in the form of radiation detection monitors, training and communications support to extract alarm data from the integrated systems and to provide it to the host country and CSI officials for evaluation.

The key to the successful incorporation of an integrated cargo inspection concept into the Megaports Initiative framework will be the agreement by the private terminal operators and host government officials that radiation alarms will be properly assessed and resolved prior to containers departing the port. The completion of agreements between the U.S. Department of Energy and the appropriate host government agency on data sharing for alarm evaluation and response will remain a critical element to the long-term success of this effort.

Partnership with DNDO

Because the SLD program provides a critical layer in the global nuclear detection architecture, NNSA and DNDO's cooperation in the campaign to reduce the threat of nuclear terrorism is crucial. We are working closely with DNDO to identify areas where the SLD program can make the external layer of the Global Architecture more robust, including the possibility of partnering with the private sector. Given that we are both involved in the deployment of radiation detection equipment, our offices routinely exchange programmatic and technical information and are working collaboratively to establish requirements for future systems. As I stated earlier, we expect DNDO's operational testing and evaluation of improvements in nuclear detection equipment will greatly benefit our international deployment

efforts. We also plan to take advantage of DNDO's procurement efforts and will seek to purchase ASP and upgraded hand-held detectors through their contract vehicles. I believe this is a mutually beneficial relationship and that we will continue to experience constructive exchanges with DNDO.

In closing, I would like to restate that the NNSA/SLD Program is dedicated to preventing the smuggling of nuclear and radiological material at international seaports, airports and land border crossings. We accomplish this goal by working closely with foreign governments and by maintaining strong relationships with other agencies and departments in the U.S. Government. We firmly believe that the unique capabilities of each Department and agency are being leveraged to accomplish our common objective of preventing nuclear material from reaching the shores of the United States.

Thank you. At this point, I would be happy to answer any questions.

The Nuclear and Radiological Threat: Securing the Global Supply Chain

Opening Statement

of

Mr. Vayl S. Oxford
Director
Domestic Nuclear Detection Office
Department of Homeland Security

Before Senate Committee on Homeland Security and Governmental Affairs
Permanent Subcommittee on Investigations

March 28, 2006

Introduction

Good morning, Chairman Coleman, Ranking Member Levin and distinguished members of the subcommittee. I am Vayl Oxford, the Director of the Domestic Nuclear Detection Office (DNDO), and it is my pleasure to come before you today to discuss how we are responding to the threat of nuclear or radiological terrorism. I would like to thank the committee for the opportunity to share the progress we are making at DNDO and within the Department of Homeland Security (DHS).

Today, I will discuss several topics related to the use of technology to detect nuclear and radiological materials that could be used in a terrorist attack. I will review DNDO accomplishments in the past year, some of our program priorities for the upcoming years, and key, long-term challenges that we face. I will specifically touch upon the progress we have made with Customs and Border Protection (CBP) regarding the deployment of Radiation Portal Monitors (RPMs) at U.S. ports of entry (POEs), and how DNDO, and DHS as a whole, is considering innovative ideas like the Integrated Container Inspection System, or ICIS, which is being piloted at the Hong Kong Modern Terminal.

Before describing our efforts, I would like to point out that protecting the United States from nuclear threats is a job that extends beyond the work of DHS, and I would like to thank our partners, in particular the Department of Energy (DOE) and CBP, who are here with me today, as well as the Departments of Defense (DOD) and State, the Federal Bureau of Investigation (FBI), and the Nuclear Regulatory Commission (NRC) for their tireless dedication to this mission and for their contributions to our interagency office.

DNDO Founding, Accomplishments, and the Road Ahead

Combating the threat of catastrophic destruction posed by terrorists possessing nuclear or radiological weapons is one of the most critical priorities of not only DHS, but the U.S. Government. In order to integrate the Department's efforts against this threat under a singular direction, as well as coordinate these efforts with relevant partners across the government, Secretary Chertoff provided notification, in accord with Section 872 of the Homeland Security Act, of his

intent to establish the DNDO to the Senate Committee on Homeland Security and Government Affairs on April 13, 2005.

On April 15, 2005, the President signed a joint presidential directive NSPD-43/HSPD-14, "Domestic Nuclear Detection," establishing the office. DNDO was assigned the responsibility to direct nuclear and radiological detection technology development programs, and serve as the focal point of all radiological detection research and development collaboration between DHS, DOE, and other related Federal agencies. Full-time detailees from these agencies have since solidified our working relationship through their participation in all aspects of the DNDO mission.

In the short time since its founding, the DNDO has taken major steps towards achieving its stated mission. We completed the first ever global nuclear detection architecture analysis that identified vulnerabilities and priority initiatives across Federal, State, and local governments. The architecture study was completed four months ahead of schedule and briefed to partner agencies and the White House in October and November of 2005. This architecture effort was funded and led by DNDO, but involved considerable interagency participation to deliver a consensus strategy to be implemented across the Federal government.

It should be noted that the DNDO will not be responsible for implementing all, or even most, elements of the proposed architecture. We are responsible for implementing domestic components, but will work with other agencies, to include DOD, DOE, State, and the Department of Justice, to ensure the implementation of the entire architecture. In particular, the DNDO has been working with the DOE in the development of the international portion of the global architecture, which incorporates DOE programs such as Second Line of Defense. We are also in ongoing discussions about how next-generation detectors developed by DNDO may be deployed through the Megaports Initiative. As previously mentioned, full-time detailees from agencies such as DOE enable us to maintain an open and productive dialogue with our partners so that we may make strides towards the complete implementation of the proposed architecture.

Other accomplishments include our acceleration of several technology development programs. We have completed the initial engineering development phase of the Advanced Spectroscopic Portal, or

ASP, program. This system development and acquisition program is improving current generation radiation portal monitors with the ability not only to detect the presence of radiation, but to identify the materials causing the alarms so that we can dismiss non-threatening sources. This enhanced capability will provide significant improvement for CBP secondary inspection operations, as well as greatly reduce secondary referral rates when operated as a means of primary inspection. Last fall, these engineering development programs culminated in the first ever high fidelity test and evaluation campaign to measure the true improvement in performance provided by these next-generation systems. The test data collected is now being used to support the selection of up to five vendors that will begin low-rate initial production, or LRIP. Additionally, these vendors will continue the development of the technology so we can deliver enhanced capabilities and additional design variants for unique operational venues. Twenty-four of the ASP LRIP units will be delivered to CBP for operational test and evaluation in the fall of this year, with full-rate production expected to begin in early 2007.

We have recently begun the Cargo Advanced Automated Radiography System, or CAARS, development program to deliver imaging systems that will automatically detect, within cargo, high-density material that could be used to shield threat materials from detection by radiation portal systems like ASP. The automated image processing techniques envisioned for CAARS will also substantially improve throughput rates over current generation radiography systems. These improved throughput rates will, in turn, enable CBP and other operators to effectively scan a much higher portion of cargo. The DNDO vision is to ultimately deploy ASP and CAARS systems together to ensure our ability to detect either unshielded or shielded materials across the entire threat spectrum.

While cargo security remains one of our top priorities, the DNDO is also taking steps to improve nuclear detection capabilities within our Nation's borders. We have launched the Southeast Transportation Corridor Pilot program to deploy radiation detectors to truck weigh stations and other sites. These deployments will be at locations agreed to by our regional partners in accordance with the domestic detection architecture developed by the DNDO. Included in the pilot program will be the necessary training, technical reachback and operational protocols to ensure that detection

technology is being operated properly and that alarms are escalated as appropriate. I will speak more about this alarm escalation process shortly.

We are also launching a "Securing the Cities" initiative aimed at enhancing protection and response capabilities in and around the Nation's highest risk urban areas. Starting with New York City, we will work with State and local officials to develop urban and regional deployment and operations strategies, identify appropriate detection equipment, establish the necessary support infrastructure, and develop incident management protocols to respond to a small scale "dirty bomb" attack.

These two initiatives, when integrated, form the basis for the DNDO vision for an interior layer nuclear detection framework. As these initiatives mature, the lessons learned will be exported to other regions and cities to enhance our overall preparedness against nuclear and radiological threats. Moreover, we offer assistance to State and local officials developing grant applications, ensuring that short-term detection pilots support long-term capabilities.

The DNDO plans to support the training of approximately 1,500 State and local operators in the use of rad/nuc detection equipment through fiscal year 2007. Our collaborative partnership with the DHS Office of Grants and Training allows us to administer funds and oversee the design, delivery, evaluation, and continual improvement of preventative rad/nuc training curriculum. Because of the varying levels of resident expertise encountered in State and local venues, the DNDO has developed a modular training curriculum that can be easily and rapidly tailored to the appropriate audience. The training modules span a range of topics, and currently include modules that cover "radiation 101," nuclear threat awareness, response protocols and specific equipment operation. As State and local operations increase, the DNDO will continue to work with the DHS Office of Grants and Training to deliver additional training options, such as "radiation detection for commercial vehicle inspection" or "radiation detection surge programs."

The DNDO is also working with the State and local community, as well as nuclear experts in the National Labs, to establish regional technical reachback capabilities to support their operations. As alarms escalate, this program will provide technical expertise to operators to ensure that alarms are resolved properly or, if necessary, that alarms are elevated to the appropriate response assets. As

part of this support effort, the DNDO recently completed the development of a comprehensive U.S. Government process for alarm resolution that brings our procedures in line with the drastically altered security environment that we now face. This new alarm resolution process represents the first restructuring of the Federal alarm resolution and response protocols in over a decade.

Even with all of the accomplishments I have outlined, there are still key, long-term challenges and vulnerabilities in our detection architecture that require a well-supported research and development program. These challenges include detecting threat materials from greater distances, in highly cluttered backgrounds, or in the presence of shielding and masking materials. We are launching initiatives to develop technologies to meet these challenges, as well as commencing a broad basic research program across private industry, National Labs, and academia to stimulate the entire field of nuclear detection sciences.

RPM Deployment Strategy

This committee has expressed particular interest in the progress of RPM deployment at U.S. POEs. I would like to take the opportunity to address this topic in detail.

In its report entitled, "Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain," the Government Accountability Office (GAO) recommended that the "the Secretary of Homeland Security working with the Director of DNDO, in concert with CBP and Pacific Northwest National Laboratory, or PNNL, devise a plan to close the gap between the current deployment rate and the rate to complete deployments by September 2009." DNDO concurred with this recommendation and now proposes a deployment strategy that will result in screening 98% of all containerized cargo crossing the southern border by fiscal year 2006 and at seaports by fiscal year 2007. This strategy will result in full coverage of all incoming containerized cargo by the end of fiscal year 2011.

In this same report, the GAO also recommended that "once cost and capabilities of advanced technology portal monitors are well understood, and before any new equipment is purchased, the Secretary of Homeland Security will work with the Director, DNDO to analyze the benefits and

costs of deploying advanced portal monitors." Again, we fully concur with the need for a deliberate process to ensure that public funds are used in a responsible manner, and that ASP systems, which do have a higher initial procurement cost, are deployed in a cost-effective manner. DNDO testing of ASP systems at the Nevada Test Site has since validated the systems' spectroscopic capabilities when compared with plastic-based systems and demonstrated, in some cases, a four-fold improvement in performance against threat-like objects and a 60% reduction in nuisance alarms generated by naturally occurring radioactive materials (NORM).

This information is now guiding a joint DNDO-CBP analysis in support of a revised RPM deployment strategy that is an optimized mix of current- and next-generation technologies, balancing our need for better capability with coverage concerns and their associated costs. This new joint deployment strategy is predicated on placing ASP systems at the highest throughput ports, where reductions to secondary inspection rates will have the greatest benefit. Current-generation systems will continue to be deployed to lower volume ports, where operations can be easily sustained while still meeting detection threshold requirements. Initial results of this analysis support the decision to acquire over 600 detection units in fiscal years 2006 and 2007, including 184 current-generation RPMs and 106 next-generation portal systems this year, and 131 current-generation and 142 next-generation systems in fiscal year 2007.

As I have mentioned, the DNDO relies heavily on the ability to obtain high fidelity, defendable test data in support of development, acquisition, and deployment decisions. DNDO testing activities are conducted throughout the product development process, and involve the National Labs, private industry and academia. The construction of the DNDO Radiological and Nuclear Countermeasures Test and Evaluation Complex (Rad/NucCTEC) is expected to be complete this September and will offer the opportunity for further high-fidelity test and evaluation. The facility will provide the capability for handling of special nuclear material, or SNM, for the purpose of testing technologies against actual samples of materials that could be readily used in a nuclear attack. Until the construction of this facility, no location existed which allowed access to SNM while maintaining the flexibility to place these materials into relevant threat scenarios and cargo configurations. Through the Rad/NucCTEC, the DNDO will be able to gather performance data and conduct independent evaluations of prototypes and products in support of a fair and open acquisition process.

It is our belief that this testing environment, one which provides access to realistic threat scenarios in the spirit of independent assessment, provides a unique opportunity. While there are radiological and nuclear detection technology test activities at PNNL, Sandia, and Brookhaven National Laboratories, none currently have access to the quantities of materials available at the Rad/NucCTEC. The National Labs certainly possess other testing capabilities, such as the environmental test chambers at Oak Ridge National Laboratory. Therefore, the DNDO hopes to leverage, not duplicate these capabilities. Experts from the National Labs and the National Institute of Standards and Technology have and hopefully will continue to be members of the DNDO test teams. They help us scope our tests, conduct data analysis, and provide support personnel for operational evaluations at the DHS Science & Technology Countermeasures Test Beds. They have also worked with us on pilot deployments for CBP, as is the case with PNNL.

Integrated Cargo Inspection

While we have made great progress in the first year of our existence, including crafting a comprehensive strategy for technology development and deployment, the DNDO continues to aggressively seek innovative approaches to nuclear detection. Members of this committee traveled to Hong Kong this past December and were able to see a pilot project at the Hong Kong Modern Terminal called the Integrated Container Inspection System, or ICIS.

I would like to applaud the private sector for creating new concepts for screening international containers like ICIS. Private sector container screening can be compatible with the U.S. Government's layered security strategy, and is another tool to further our ability to identify and address risks in an expedited manner. An integrated cargo inspection system, one that combines targeting, passive detection, radiographic imaging and information analysis would be a robust solution to the nuclear and radiological detection challenges that we face.

The ICIS pilot at Hong Kong Modern Terminal demonstrates potential interest in private sector acquisition and operations of container screening technologies. It is a model for comprehensive passive and active inspection, as well as a model for public-private partnership. However, ICIS, as

deployed, is not an operational system. It utilizes currently available technology that is not optimized for radiation detection. DHS has sent teams to observe the ICIS pilot and determined that the technology they have used has potential, but still faces significant limitations.

If ICIS, as it exists, is not a complete solution for nuclear detection, then what type of system do we think we need? The DNDO certainly favors an integrated system approach. At international seaports, every cargo container should be both passively and radiographically scanned. This would enable us to detect unshielded or lightly shielded materials with current and next-generation RPMs like ASP, as well as automatically detect highly-shielded threat materials using a radiographic scanner like CAARS. Detector data should be analyzed by the U.S. Government prior to cargo transit, with the CBP Automated Targeting System (ATS), manifest and detector data integrated for enhanced targeting capability. Additional targeted inspection utilizing mobile advanced RPMs with radiography systems could be performed upon arrival at a POE. Proposed approaches could include public-private partnerships with the mandate that the U.S. Government would receive all raw data streams.

As we strive towards the goal of full coverage, we must not lose sight of our ultimate goal – protecting this Nation against nuclear and radiological terrorism. Private sector screening of international cargo could further enable DHS' ability to resolve security concerns related to identified high risk containers. However, such efforts must supplement, not replace, the need for advance data reporting and targeted inspection at our POEs.

Conclusion

In conclusion, the DNDO is taking a comprehensive approach to addressing the threat posed by a terrorist nuclear attack. This approach, which begins with focused research and development programs that culminate in high fidelity test and evaluation campaigns, provides the basis for the Department to make informed and justifiable acquisition decisions. Equally important is the recognition on behalf of DNDO that the successful deployment of these technologies must be done as part of a larger strategy, one that extends to deployments executed by other agencies. Ultimately,

all of these systems must be connected and work within an environment that responds to information obtained from intelligence, counterterrorism, and law enforcement communities.

I am proud to have shared with you today how DNDO and its partners are continuing to make progress against this very real threat. I look forward to working with you on this subcommittee in an ongoing effort to protect the Nation.

This concludes my prepared statement. With the committee's permission, I request my formal statement be submitted for the record. Chairman, Senator Levin, and Members of the Subcommittee, I thank you for your attention and will be happy to answer any questions you may have.

Efforts to Detect and Interdict Radiological or Nuclear Material

Statement

of

JAYSON P. AHERN

ASSISTANT COMMISSIONER

OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS & BORDER PROTECTION

Hearing Before Senate Committee on Homeland Security
and Governmental Affairs
Permanent Subcommittee on Investigations

MARCH 28, 2006

Good afternoon Chairman Coleman, Ranking Member Levin and distinguished member of the subcommittee. I am Jayson Ahern, Assistant Commissioner, Office of Field Operations, U.S. Customs & Border Protection (CBP). It is a privilege to appear before you today and I thank you for this opportunity to discuss the CBP programs that are fundamental to securing our ports of entry from the threat of nuclear terrorism.

First of all, let me assure you that preventing the smuggling of illicit nuclear weapons and radiological materials remains CBP's highest priority. Since my last testimony before this committee, CBP has made significant strides in its priority plan for the deployment of radiation detection equipment. Although the focus of this hearing is on our radiation detection equipment at our nation's borders, CBP employs a multi-layered defense strategy and works with the Intelligence Community to substantially increase the likelihood that nuclear or radiological material will be detected.

CBP has integrated its radiation detection technology deployment initiative into its multi-layered defense strategy to address the threat of nuclear and radiological terrorism that begins outside the United States where the movement of illicit nuclear and radiological materials is initiated and continues all the way to the U.S. borders.

CBP, as the guardian of the Nation's borders, safeguards the homeland - foremost, by protecting the American public against terrorists and the instruments of terror; while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Contributing to all this is CBP's time-honored duty of apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties, and enforcing U.S. trade laws.

In fiscal year 2005, CBP processed over 431 million passengers, more than 121 million land border passenger vehicles, 1 million aircraft, 113,325 vessels, and over 25 million sea, rail and truck containers. In fiscal year 2005, CBP made 22,727 arrests and 23,802 narcotic seizures; seized over 798,000 pounds of narcotics, approximately $28 million in currency, and over $120 million in merchandise. We cannot protect against the entry of terrorists and the instruments of terror without performing all missions.

We must perform all missions without stifling the flow of legitimate trade and travel that is so important to our nation's economy. We have "twin goals" - building more secure and more efficient borders.

Meeting Our Twin Goals - Building More Secure and More Efficient Borders:

As the single, unified border agency of the United States, CBP's missions are extraordinarily important to the protection of America and the American people. In the aftermath of the terrorist attacks of September 11th, CBP has developed initiatives to

meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. Our homeland strategy to secure and facilitate cargo moving to the United States is a layered defense approach built upon interrelated initiatives. They are: the 24-Hour and Trade Act rules, the Automated Targeting System (ATS), housed in CBP's National Targeting Center, the use of Non-Intrusive Inspection equipment and Radiation Portal Monitors, the Container Security Initiative (CSI), and the Customs-Trade Partnership Against Terrorism (C-TPAT) initiative. These complementary layers enhance seaport security, and protect the nation.

Advance Electronic Information:

As a result of the 24-Hour rule and the Trade Act, CBP requires advance electronic information on all cargo shipments coming to the United States by land, air, and sea, so that we know who and what is coming before it arrives in the United States. The 24-Hour Advanced Cargo Rule requires all sea carriers, with the exception of bulk carriers and approved break-bulk cargo, to provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port for shipment to the United States. Failure to meet the 24-Hour Advanced Cargo Rule results in a "do not load" message and other penalties. This program gives CBP greater awareness of what is being loaded onto ships bound for the United States and the advance information enables CBP to evaluate the terrorist risk from sea containers on 100% of shipments.

Automated Targeting System:

The Automated Targeting System, which is used by the National Targeting Center and field targeting units in the United States and overseas, is essential to our ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are "high risk," and should be scrutinized at the port of entry, or in some cases, overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

The National Targeting Center, working closely with the Coast Guard, also vets and risk scores all cargo and cruise-ship passengers and crew prior to arrival. This ensures that DHS has full port security awareness for international maritime activity.

Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT) - Extending our Zone of Security Outward & Partnering with Other Countries:

In fiscal year 2005, over 11.3 million seagoing containers arrived at our nation's seaports. Another 11.3 million cargo conveyances arrived by land. About 90% of the world's manufactured goods move by container, much of it stacked many stories high

on huge transport ships. Each year, two hundred million cargo containers are transported between the world's seaports, constituting the most critical component of global trade. The greatest threat to global maritime security is the potential for terrorists to use the international maritime system to smuggle terrorist weapons – or even terrorist operatives – into a targeted country.

Clearly, the risk to international maritime cargo demands a robust security strategy that can identify, prevent and deter threats, at the earliest point in the international supply chain, before arrival at the seaports of the targeted country. We must have a cohesive national cargo security strategy that better protects us against the threat posed by global terrorism without choking off the flow of legitimate trade, so important to our economic security, to our economy, and, to the global economy.

We developed a layered enforcement approach that addresses cargo moving from areas outside of the United States to our ports of entry. Our approach focuses on stopping any shipment by terrorists before it reaches the United States, and only as a last resort, when it arrives at a port of entry.

The Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) initiatives bolster port security. Through CSI, CBP works with host government Customs Services to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on-board vessels destined for the United States. In addition to the current 44 foreign ports participating in CSI covering 75% of maritime containerized cargo shipped to the U.S., many more ports are in the planning stages. By the end of 2006, we expect that 50 ports, covering 82% of maritime containerized cargo shipped to the U.S. will participate in CSI.

Through C-TPAT, CBP establishes voluntary best security practices for all parts of the supply chain, making it more difficult for a terrorist or terrorist sympathizer to introduce a weapon into a container being sent by a legitimate party to the United States. C-TPAT covers a wide variety of security practices, from fences and lighting to requiring that member companies conduct background checks on their employees, maintain current employee lists, and require that employees display proper identification.

C-TPAT's criteria also address physical access controls, facility security, information technology security, container security, security awareness and training, personnel screening, and important business partner requirements. These business partner requirements encourage C-TPAT members to conduct business with other C-TPAT members who have committed to the same enhanced security requirements established by the C-TPAT program.

The C-TPAT program has created a public-private and international partnership with nearly 5,800 businesses (over 10,000 have applied), including most of the largest U.S. importers. Forty-five percent of all merchandise imported into the United States is done so by C-TPAT member importers. C-TPAT, CBP and partner companies are working together to improve baseline security standards for supply chain and container security. CBP reviews the security practices of not only the company shipping the goods, but also the companies that provided them with any services.

The validation process employed by CBP demonstrates and confirms the effectiveness, efficiency and accuracy of a C-TPAT certified member's supply chain security. At present, the C-TPAT program has completed validations on 27 percent (1,545 validations completed) of the certified membership, up from 8 percent (403 validations) completed a year ago. Additionally, validations are in progress on another 39 percent (2,262 in progress) of certified members, and these validations will be completed throughout 2006, bringing the total percentage of certified members to 65 percent by year-end. In 2007, the C-TPAT program validations will continue. We will have validated 100 percent by the end of CY 2007.

Additionally, CBP has moved to tighten minimum-security criteria for membership in this voluntary program. Working closely with the trade community and key stakeholders, CBP has developed and implemented baseline security standards for member importers, sea carriers, and highway carriers. CBP will complete this process by the end of CY 2006, defining the minimum-security criteria for the remaining enrollment sectors – air carriers, rail carriers, brokers, freight forwarders, and foreign manufacturers.

In order to promulgate security best practices, C-TPAT recently compiled and published a best practice catalog, which was distributed to all members and made available at its recent training seminar. Each year C-TPAT conducts an annual seminar providing additional security training and presentations from the trade community on how implementation of C-TPAT has improved their security and provided a measurable return on investment. C-TPAT will also be implementing a discussion board available on their secure web portal whereby members can exchange ideas and discussions on security practices and benefits.

Non-Intrusive Inspection Equipment and Radiation Detection Portals:

CBP also uses cutting-edge technology, including large-scale X-ray and Gamma-ray Non-Intrusive Inspection (NII) systems to image cargo, and radiation detection devices to screen cargo for the presence of radiological materials.

Since CBP was formed in March 2003, we have increased our large-scale NII inventory by 60 systems, including 19 additional systems to the northern border, 16 additional systems to the southern border and 25 additional systems to seaports. CBP currently has an inventory of 171 large-scale NII systems deployed nationwide.

In fiscal year 2005, CBP examined nearly 80 percent of all rail cars, nearly 25 percent of all land conveyances, and 5 percent of all sea-borne containers that arrived in the U.S. The majority of these examinations were accomplished with the use of large-scale NII technology. At a minimum, 100 percent of all high-risk conveyances are imaged with large-scale NII technology and screened with a hand-held Radiation Isotope Identifier Device for the presence of radiation. Approximately 2 million examinations were conducted with large-scale NII technology at our nation's ports of entry prior to 2003. In fiscal year 2005, that number increased to 5.4 million. Since March 2003, large-scale NII technology has been used to conduct approximately 12 million examinations.

Since March 2003, in addition to large-scale NII technology, CBP has deployed an additional 709 Radiation Portal Monitors (RPM), 299 Radiation Isotope Identifier Devices (RIID) and approximately 5,500 Personal Radiation Detectors (PRD) to our ports of entry.

CBP currently operates 740 RPMs at our nation's ports, including 190 RPMs at seaports. RPMs are our most robust radiation detection devices that provide CBP with a passive non-intrusive means to quickly and thoroughly screen conveyances and/or shipments for the presence of illicit radiological materials. CBP has also deployed a total of 491 RIIDs and approximately 12,500 PRDs to our nation's ports of entry.

CBP currently screens 100 percent of mail and express consignment packages, 90 percent of all containerized cargo and 80 percent of all privately owned vehicles entering the U.S. along the Northern Border, 90 percent of all containerized cargo and 79 percent of all privately owned vehicles entering the U.S. along the Southern Border, and 44 percent of all arriving sea-borne containers for the presence of radiation with RPMs.

Overall, CBP currently screens approximately 67 percent of all arriving land/sea containerized cargo entering the United States with RPMs. That number will continue to grow through the remainder of this year and 2007. CBP will deploy a total of 621 RPMs to our Nation's top seaports, which will allow us to screen approximately 98 percent of inbound sea-borne containers by December 2007. A portion of these deployed systems will be next-generation Advanced Spectroscopic Portals, which will begin to be deployed in mid-FY 2007. In addition, CBP will deploy 60 Mobile RPM Systems to seaports in 2006. Mobile RPMs will provide us with the flexibility to conduct screening operations at low-volume locations and to screen high-risk containers in a real-time fashion. Initial deployment of the Mobile RPMs will occur in April with all 60 expected to be in place by the end of CY2006. CBP's ultimate goal is to screen 100 percent of all high-risk people, cargo and conveyances for radiation.

CBP has strict response protocols in place to address and resolve all radiation alarms. If our field officers require assistance in resolving a radiation alarm, technical reach-back support is available 24 hours a day 365 days a year. Our Laboratories and Scientific Services (LSS) scientists located at the National Targeting Center provide that support. Beyond this support, further technical assistance is available through the DNDO Secondary Reachback program, which provides access to the nuclear design and spectroscopy expertise resident in the National Laboratories.

To date, CBP has screened over 80 million conveyances with RPMs. Radiation-screening results are shared with other Federal agencies as well as certain State and Local entities as appropriate. The total number of gamma and/or neutron-related radiation alarms to date is over 318,000. However, all alarms have been resolved and the overwhelming majority has been attributed to naturally occurring radioactive materials (NORM) or medical patients. Thus far, no RPM alarms have been attributed to the illicit transport of special nuclear material.

Also, over 600 canine detection teams, capable of identifying narcotics, bulk currency, human beings, explosives, agricultural pests, and chemical weapons, are deployed at our ports of entry.

CBP Coordination with DNDO:

In addition to increased screening efforts at our own ports of entry for radioactive and nuclear materials, the DHS Domestic Nuclear Detection Office (DNDO) fully endorses the concept of increased active and passive detection at foreign ports of departure. Foreign ports can also use the systems DNDO are acquiring and developing with a CSI presence, as well as the Department of Energy's Megaports program. We must continue to stress the need for increased screening at foreign ports of departure; while at the same time have a robust screening effort at our own ports of entry.

The DNDO FY 2007 budget request of nearly $536 million includes $157 million for the acquisition and deployment of current and next-generation radiation detection systems at our ports of entry. These systems will be deployed and operated by CBP. In addition, DNDO's FY 2007 budget also includes funding for the development of enhanced cargo radiography screening systems for our ports of entry. CBP will continue to work closely with DNDO to explore new and emerging technologies in an effort to enhance our antiterrorism capabilities. These enhanced screening efforts will complement the many information-based programs CBP already has in place for enhanced port security.

Integrated Container Inspection System (ICIS):

DHS and CBP acknowledge that the Hong Kong Container Terminal Operators Association (HKCTOA) and Science Applications International Corporation (SAIC) have taken an important step forward in an effort to improve container security. The Integrated Container Inspection System (ICIS) pilot demonstrates that the concept of collecting and integrating radiation detection spectral data with radiographic imaging on containers departing Hong Kong is complementary and consistent with our agency's goals.

As the HKCTOA continues to make progress in collecting valuable screening data, CBP remains committed to working with the Association, the Hong Kong Customs & Excise Department and the Hong Kong Government to develop the policies, procedures and response protocols that will allow us to take full advantage of the investment the Hong Kong shipping community is making to better protect maritime trade and the global supply chain.

CBP and DNDO meet regularly to discuss potential implementation strategies. Results from the ongoing analysis will impact future discussions.

Government Accountability Office Findings:

Recently, the Government Accountability Office (GAO) submitted a report entitled "Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation

Detection Equipment at U.S. Ports of Entry, but Concerns Remain." The report contained several recommendations for improvement. In addition to the report, GAO investigators were also tasked with examining possible weaknesses in CBP's ability to detect radiation at two land border ports of entry. While the radiation detection equipment worked properly and our officers followed established CBP radiation response protocols, a recommendation was submitted to CBP.

CBP agrees with the GAO findings and will incorporate their recommendations to further strengthen our radiation detection program.

Based on the GAO recommendations, CBP will work in coordination with DNDO to:

1. Develop a plan to close the gap between the current RPM deployment rate and the rate to complete the RPM deployments by September 2009
2. Analyze the benefit and costs of deploying advanced portal monitors
3. Continue developing procedures for screening rail containers
4. Revise our standard operating procedures to stress that whenever a secondary RPM alarm cannot be resolved with an external radiation detection technology examination, an officer will open the container in an attempt to resolve the alarm
5. Implement a procedure whereby CBP officers can verify the authenticity of a Nuclear Regulatory Commission license
6. Ensure that Pacific Northwest National Laboratory certifies their value management system

Conclusion:

In summary, as I have previously noted, CBP screens 100% of containers for risk. All containers that CBP determines to be of risk are examined using a variety of technologies, either at the foreign port of loading under the Container Security Initiative, or upon arrival into the U.S. port of entry. The technologies used include radiation screening, non-intrusive x-ray inspection, and as appropriate, physical examination. CBP officers tasked with the security of our seaports carry out this screening and examination.

Mr. Chairman, Members of the Subcommittee, I have briefly addressed CBP's critical initiatives today that will help CBP protect America against terrorists and the instruments of terror, while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. With the continued support of the President, DHS, and the Congress, CBP will succeed in meeting the challenges posed by the ongoing terrorist threat and the need to facilitate ever-increasing numbers of legitimate shipments and travelers.

Thank you again for this opportunity to testify. I will be happy to answer any of your questions.

TESTIMONY OF

DEPUTY SECRETARY MICHAEL P. JACKSON

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

MARCH 30, 2006

Chairman Coleman, Ranking Member Levin, and members of the subcommittee, I am pleased to be here today to discuss the critically important issue of global supply chain security.

Secretary Chertoff has repeatedly spoken about the importance of using risk-based assessments to focus our efforts on threats that present the greatest consequences. It is not possible to eliminate all risk, but we must focus on the highest risks with tenacity and creativity. Clearly, defending against the use by terrorists of weapons of mass destruction (WMD), particularly radiological and nuclear devices, is the highest priority of our maritime cargo security efforts.

Mr. Chairman, this subcommittee and the full Committee have been consistently focused on these issues, and committed to innovation. I want to assure you that the Department of Homeland Security (DHS) shares your commitment to strengthen supply chain security. I am personally committed to nurturing a healthy dose of urgency within DHS to deliver continuous improvement in this area. We can afford no less.

Since September 11, 2001 we have, however, made transformational improvements in the extent and quality of the layered system of systems now deployed to strengthen cargo security. This year, the DHS will spend some $2.5 billion on maritime security. Overall, the Federal Government is spending $2.9 billion, including the Department of Energy's Megaports program. If the President's FY 07 budget is enacted, we will have spent some $9.6 billion in this area in four years (FY04-FY07). Earlier this week, colleagues from Customs and Border Protection (CBP), DHS' Domestic Nuclear Detection Office, and the Department of Energy testified to you about this work and the tools we have already put in place. So I'll try not to duplicate the detailed testimony they provided.

We could not have come this far without the full engagement and serious commitment of thousands of private sector partners around the globe. Representatives of several organizations and businesses participating closely in this work will testify later today. DHS is grateful for their shared commitment to secure the supply chain.

Although we have made great progress, more needs to be done. In fact, we must be institutionally disciplined to understand that our commitment to stay ahead of those who would do harm to our people and our economy can never cease. Terrorists will continue to probe our systems and will themselves innovate. Still a young organization, DHS must operate every day with urgency and discipline, while casting our eyes to the future.

Today I'd like to talk particularly about the path ahead to strengthen security for the global supply chain. I will focus on the WMD threat because of its centrality, but will also touch on measures that will also strengthen our ability to detect all forms of contraband. Secretary Chertoff has launched the Secure Freight initiative to implement aspects of the work ahead for DHS and the industry.

A Layered System of Systems Supporting a Global Network. First, a brief word about our overall approach to supply chain security. Our security doctrine is grounded upon a commitment to deploy a strong, layered system of security systems. By deploying multiple, mutually reinforcing security layers and tools, we diminish the risk associated with failure at a single point. Some layers may have a more immediate and obvious security function, such as the physical inspection of a container by CBP field agents. Others, such as the Administration's work in global nuclear non-proliferation are complimentary, aimed at making it more difficult to acquire WMD components. Security is very seldom adequately delivered via a single silver bullet.

It begs the obvious, but bears noting, that we are talking about a *global supply chain* that serves an *interdependent global economy*. Thus, a second doctrinal component of our cargo security strategy has been, where possible, to push security measures out beyond our borders. It has required close partnerships with the private sector, because they own most of the assets and move the goods. As the recent debate about the now abandoned DP World transaction within the United States underscores, the basic facts about who owns and operates the global supply chain can cause concerns.

With whom should we partner and how? A fair question. But there is no question that we must partner to ensure both security *and* mobility. CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) is an example of such a partnership program. Here, the aphorism made famous by President Reagan guides: trust but verify. C-TPAT's verification regime is an example of our doing that.

It strengthens our hand to partner closely with other governments, which is why bilateral and multilateral solutions to supply chain security have been a focus for this Administration. The Container Security Initiative and our work with the World Customs Organization, the International Maritime Organization and the International Standards Organization have improved security.

Some of the first generation layers of security will give way to second-generation tools. Others will be strengthened. New tools will be added. Not all of the layers are

appropriately unpacked in public hearings. But perhaps it would be useful simply to lay out the basic structures for supply chain security and elaborate on those areas that I consider most ripe for accelerated improvement.

Existing Security Architecture. An outline of the existing security architecture includes four core components: (1) vessel security; (2) personnel security; (3) cargo security; and (4) port facility security. Some elements of each of these four components are focused abroad, others at home – thus there are essentially eight buckets of activity that capture most of the programmatic focus of the supply chain security challenge.

Most of the core federal programs were explained in detail by DHS testimony earlier this week. I'd just supplement that testimony with a quick overview of the Coast Guard's role in securing the supply chain at home and abroad. Their implementation of the Maritime Transportation Security Act (MTSA) in the United States and the International Ship and Port Facility Security (ISPS) Code abroad forms the basis for securing the foreign and domestic ports and vessels that are the foundation of the international marine transportation system.

At home, the Coast Guard routinely inspects and assesses the security of 3,200 regulated facilities in more than 360 U.S. ports at least annually in accordance with MTSA and the Ports and Waterways Security Act. Every regulated U.S. port facility, regardless of owner/operator, is required to establish and implement a comprehensive Facility Security Plan that outlines procedures for controlling access to the facility, verifying credentials of port workers, inspecting cargo for tampering, designating security responsibilities, training, and reporting of all breaches of security or suspicious activity, among other security measures. Working closely with local port authorities and law enforcement agencies, the Coast Guard regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance.

In accordance with MTSA, the Coast Guard has completed verification of security plans for U.S. port and facilities and vessels operating in U.S. waters. Specifically,

- Port Threat Assessments for all 55 militarily or economically critical ports have been completed. The Coast Guard has developed 44 Area Maritime Security Plans covering 361 ports, the Great Lakes, the Inland and Western Rivers and the Outer Continental Shelf region.
- The Coast Guard completed initial security plan verification exams on all 6,200 U.S. flag inspected vessels on July 1, 2005.
- The Coast Guard has completed 2,400 verification examinations on un-inspected vessels regulated under the MTSA, and is on track to complete all 4,800 by December 31, 2006.

In addition, the Automatic Identification System has been fielded at 9 ports with Vessel Traffic Service systems and allows the Coast Guard to identify and track vessels in the coastal environment. Long range tracking, currently in development, will enable the

Coast Guard to identify and track vessels thousands of miles at sea, well before they reach our coastal zones. Likewise, the Inland River Vessel Movement Center provides critical information about the movement of hazardous cargoes along our nation's inland rivers.

The Coast Guard has also established 12 Maritime Safety and Security Teams and enforced hundreds of fixed and moving security zones to protect Maritime Critical Infrastructure and key assets and naval vessel protection zones to protect U.S. Navy and Maritime Administration vessels. Further, the Coast Guard is developing a risk-based decision making system, to be implemented this year, which will help prioritize high capacity passenger vessels escorts. Although initially developed for high capacity ferries, its application is being expanded to enhance current security measures for other high capacity vessels: ferries, cruise ships, and excursion vessels carrying 500 or more passengers.

Abroad, the Coast Guard conducts foreign port security assessments through its International Port Security Program. To date the Coast Guard has assessed 45 countries, with 40 having been found to be in substantial compliance with the International Ship and Port Facility Security Code. These 45 countries are responsible for over 80 percent of vessel arrivals to the United States. The five countries that are not in substantial compliance have been notified to take corrective actions or risk being placed on a port security advisory and have conditions of entry imposed on vessels arriving from their ports. The Coast Guard is on track to assess approximately 36 countries per year with an ultimate goal of visiting all of our maritime trading partners within four years.

Finally, in addition to the work of the Coast Guard, the Port Security Grant program (PSGP) has awarded over $700 million to owners and operators of ports, terminals, and U.S. inspected passenger vessels and ferries, as well as port authorities and State and local agencies to improve security for operators and passengers through physical security enhancements. These grants are intended to create a sustainable, risk-based effort for the protection of ports from terrorism, especially explosives and non-conventional threats that would cause significant loss of life and major disruption to commerce.

As part of the FY 2005 PSGP, significant changes were introduced to make the program more risk based. And it required certain grantees to supply matching funds, which added some $30 million more to this program. Changes include limiting eligibility to the nation's most at-risk seaports and distributing funding based on risk, needs and national priorities for port security.

I'd like now to focus on two particular areas that present significant upside for improving security: (1) improvements regarding DHS's targeting of containers of highest risk and tools to inspect containers; and (2) deployment of the Transportation Worker Identification Card for unescorted access to U. S. ports.

Secure Freight. The Department's Secure Freight initiative has two major components: better targeting and enhanced inspection tools.

Better Targeting. CBP's Automated Targeting System (ATS), which is used by the National Targeting Center and field targeting units in the United States and overseas, profiles inbound cargo and identifies high-risk cargo entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized at the port of entry or overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

ATS is an extraordinarily powerful "first generation" tool, and a more sophisticated, next-generation tool is under development at DHS as part of the Secure Freight initiative. ATS data is derived from filings of the cargo waybill and an extensive historical risk scoring algorithm derived from years of data about containers and inspections.

The next-generation tool will fuse existing data from across the supply chain by multiple actors who touch the box from order, container origin, to destination. The data aggregation would, in my view, best be fused by a third party intermediary – perhaps formed by the industry itself. The U.S. government would certify one or more such qualified entities formed for this purpose, and would set standards for such data fusion. The intermediary would be rigorously audited.

This approach is the natural extension of the requirement to have better data upon which to score risk of inbound containers. It would support not only the needs of the United States better to understand and assess risk of inbound containers , but also could serve the exact same needs of other nations. This is not a tool that will grow overnight. But stronger profiling is possible, and I am convinced that we can make great progress in the near term. I would welcome an opportunity to elaborate further in response to questions.

Enhanced Inspection Tools. My DHS colleagues testified already about DHS's plan to expand rapidly the number and the performance of radiation portal monitors and the next generation tool, Advanced Spectroscopic Portals. The Domestic Nuclear Detection Office has recently tested new and better handheld radiation detection equipment, which we will deploy in the marine environment.

Better detection systems can be deployed both abroad and at home. At home, our goal is to have 100 percent inspection of all containers as they depart a U.S. port headed into our country. Abroad, our goal is to increase materially the number of containers inspected by radiation detection tools and by non-intrusive inspections, including large-scale X-ray devices.

In this regard, I'd note that this week Secretary Chertoff will be in Hong Kong to see first-hand the Integrated Container Inspection System (ICIS) pilot underway there. CBP is engaged in a technical exchange to evaluate how the data gathered by ICIS can be used to strengthen our inspection capabilities. I understand that several members of this subcommittee have had the opportunity to inspect the same pilot program.

After extensive discussion with industry about the ICIS pilot and its underlying technology and business concepts, I find myself highly optimistic that this pilot can point the way to a collaborative network that can significantly enhance CBP's capabilities physically to inspect a larger number of containers from points worldwide. Again, I'd be happy to discuss with the subcommittee DHS's thought about how this might develop.

Transportation Worker Identity Card (TWIC). On Friday of this week, the Transportation Security Administration (TSA) will publish a "request for qualifications" seeking firms who are appropriately experienced and interested to help deploy certain components of the TWIC program. This is the first step toward operational deployment of the TWIC program for unescorted access to all U.S. ports. This day has been too long in coming.

This deployment will include accelerated and parallel rulemaking work by both TSA and Coast Guard. And it will include a procurement needed to help launch the operational program. Secretary Chertoff has given his team instructions to get this done as quickly as possible. Further details will be forthcoming as part of the rulemaking and procurement actions. This tool will add a valuable layer of further security to domestic port operations and will strengthen overall supply chain security.

Conclusion. The Department is working closely with other government departments and agencies, with industry, and the international community to establish workable solutions to improve supply chain security. We recognize the challenges that face our programs and the importance of protecting our nation from terrorist threats to this vital economic engine. We are making significant progress. The Department thanks you for your continued support and looks forward to working with you as these programs further develop and mature.

This completes my prepared statement. I would be happy to respond to any questions you may have.

Testimony of

Christopher Koch
President & CEO of the
World Shipping Council

Regarding

Securing Maritime Commerce and Global Supply Chains

Before the

Permanent Subcommittee on Investigations
of the
Senate Committee on
Homeland Security and Governmental Affairs

March 30, 2006

Introduction

Mr. Chairman and members of the Committee, thank you for the opportunity to testify before you today. My name is Christopher Koch. I am President and CEO of the World Shipping Council, a non-profit trade association representing international ocean carriers, established to address public policy issues of interest and importance to the international liner shipping industry. The Council's members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry roughly 93% of the United States' imports and exports transported by the international liner shipping industry, or more than $500 billion worth of American foreign commerce per year.[1]

[1] A list of the Council's members can be found on the Council's website at www.worldshipping.org.

I also serve as Chairman of the Department of Homeland Security's National Maritime Security Advisory Committee, as a member of the Departments of Homeland Security's and Treasury's Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), and on the Department of Transportation's Marine Transportation System National Advisory Council. It is a pleasure to be here today.

In 2005, American businesses imported roughly 11 million loaded cargo containers into the United States. The liner shipping industry transports on average about $1.5 billion worth of containerized goods through U.S. ports each day. In 2006, at projected trade growth rates, the industry will handle roughly 12 million U.S. import container loads. And these trade growth trends are expected to continue.

The demands on all parties in the transportation sector to handle these large cargo volumes efficiently is both a major challenge and very important to the American economy.

At the same time that the industry is addressing the issues involved in efficiently moving over 11 million U.S. import containers this year, we also must continue to enhance maritime security, and do so in a way that does not unreasonably hamper commerce.

The Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.

What is the appropriate collection of measures to address this challenge?

The Department of Homeland Security's maritime security strategy involves many different, but complementary, pieces.

It includes the establishment of *vessel security* plans for all arriving vessels pursuant to the International Ship & Port Facility Security Code (ISPS Code) and the Maritime Transportation Security Act (MTSA).

It includes the establishment of U.S. *port facility security* plans and area maritime security plans pursuant to the ISPS Code and MTSA, and the establishment by the Coast Guard of the International Port Security Program (IPSP) pursuant to which the Coast Guard visits foreign ports and terminals to share and align security practices and assess compliance with the ISPS Code.

It includes the Maritime Domain Awareness program, under which DHS acquires enhanced information about vessel movements and deploys various technologies for

better maritime surveillance. The challenge of effectively patrolling all the coasts and waters of the United States is obviously a large one.

The MTSA directives and DHS efforts also include enhanced security for *personnel* working in the maritime area.

And last, but certainly not least, these directives and efforts include an array of initiatives to enhance *cargo security* – the important topic of this hearing, including

- Cargo Security Risk Assessment Screening
- The Container Security Initiative
- The Customs Trade Partnership Against Terrorism (C-TPAT) Program, and
- Container Inspection Technology Deployment.

The liner shipping industry and the World Shipping Council have fully supported these various initiatives. Ocean carriers' business depends upon the government having a security regime that provides adequate levels of security confidence, while continuing to allow for the efficient and reliable transportation of America's exports and imports. I will now turn to the issues the Committee, in its March 13 letter of invitation, requested that my testimony address today.

Committee Question #1: The private sector perspective on U.S. government programs related to maritime and port security.

The government's multi-layer security strategy is a fundamentally sound one, and seeks to address cargo and maritime security on an international basis as early as is practicable. It does not wait to address security questions for the first time when a ship and its cargo arrive at a U.S. port. The strategy can be further developed and strengthened, however, and we appreciate the Committee's continued interest in these issues. The following is a brief description of the strategy's various layers.

A. Vessel Security

Every vessel entering a U.S. port, whether of U.S. or foreign registry, must have a ship security plan that is in accordance with the ISPS Code – a binding international convention developed under the leadership of the U.S. Coast Guard. The Coast Guard also ensures through its port state enforcement programs that vessels entering U.S. ports are in compliance with the Code. Vessels that are not in compliance are denied entry into a U.S. port by the Coast Guard.

Under MTSA, the Coast Guard requires vessels to file Notices of Arrival 96 hours before arrival in a U.S port, providing relevant advance information about the vessel, its itinerary, its crew and its cargo. The Coast Guard and Customs and Border Protection (CBP) use this information for risk profiling.

B. Port Security

Port facilities must also comply with the ISPS Code, and, in the U.S., the Coast Guard's MTSA regulations – the regulatory regime used to implement the ISPS Code domestically. All major U.S. port facilities are in compliance with the ISPS Code.[2]

These port facilities or marine terminals may be operated by the state or local government public port authority, or they may be leased from the port authority by terminal operating service providers, with the port authority maintaining ownership and oversight of the port. The majority of U.S marine terminals are operated by private marine terminal firms, which have leased the property from the port authority. Major ports generally have multiple terminals and terminal operators.

Foreign port facilities must also comply with the ISPS Code, and the U.S. Coast Guard oversees this under its International Port Security Program (IPSP). Coast Guard IPSP officers visit port facilities around the world, and feed the results from each IPS assessment into the agency's port state control security matrix, and work with the local governments if necessary to try to improve conditions if warranted.

As a way to support the Coast Guard's efforts in this regard, the World Shipping Council and Coast Guard last week formalized a voluntary reporting mechanism whereby the Council's companies can assist the Coast Guard's global maritime security efforts by reporting port facility security status issues to the Coast Guard. The intent of this effort is to provide the Coast Guard with additional information that may help the agency better prioritize its IPSP efforts, work with other governments, and enhance domestic enforcement of maritime security requirements.

C. Personnel Security

Maritime personnel security is addressed in various ways. Vessels must provide CBP and the Coast Guard with advance notice of all crew on the vessel 96 hours before the vessel arrives in a U.S port for screening. U.S. seafarers are issued credentials by the U.S. Coast Guard and must go through a security vetting process. All foreign seafarers must have valid, individual U.S. visas if they are to go ashore in the U.S.

Regarding personnel working in U.S. ports, the Department of Homeland Security has indicated that it intends to promulgate proposed rules on the Transportation Worker Identification Credential (TWIC) in the near future, as required by MTSA. At the request of DHS, the National Maritime Security Advisory Committee, after intensive, open and constructive dialogue amongst diverse industry and government officials, approved a detailed set of recommendations to the Department for its consideration in the development of this initiative. The establishment of the TWIC would help meet one of

[2] The Coast Guard's MTSA regulations estimated that the industry's compliance with the Code would cost more than $8 billion over ten years, and that figure did not include foreign port or foreign vessel compliance costs.

the unaddressed U.S. port security imperatives identified by Congress and DHS as an essential element of the nation's maritime security. The Council and its Member lines strongly support DHS promulgating a regulation on this issue. This issue remains one of the most important uncompleted tasks to improve U.S. port security.

D. Cargo Security

Particularly with respect to containerized cargo, the issues surrounding cargo security are challenges that require a multi-faceted strategy, which begins long before the cargo arrives at a U.S. port. It involves advance Customs security screening of all containers before vessel loading in a foreign port, cooperation with foreign Customs authorities through the Container Security Initiative, use of container inspection technology, and the Customs Trade Partnership Against Terrorism initiative.

a. Risk Assessment and the National Targeting Center

The stated and statutorily mandated strategy of the U.S. government is to conduct a security screening of all containerized cargo shipments *before* they are loaded on a U.S. bound vessel in a foreign port. The World Shipping Council fully supports this strategy. The correct time and place for the cargo security screening is before the containers are loaded on a ship. Most cargo interests also appreciate the importance of this strategy, because they don't want their shipments put at risk or delayed because of a security concern that could arise regarding another cargo shipment aboard the ship.

In order to be able to perform this advance security screening, CBP implemented the "24 Hour Rule" in early 2003. Under this rule, carriers are required to provide CBP with their cargo manifest information regarding all containerized cargo shipments at least 24 hours before those containers are loaded onto the vessel in a foreign port. The Council supports this rule.

CBP, at its National Targeting Center in Northern Virginia, then screens every shipment using its Automated Targeting System (ATS), which also uses various sources of intelligence information, to determine which containers should not be loaded aboard the vessel at the foreign port, which containers need to be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low-risk and able to be transported expeditiously and without further review. Every container shipment loaded on a vessel bound for the U.S. is screened through this system before vessel loading at the foreign port. Customs may issue the carrier a "Do Not Load" message on any container that is so screened if it has security concerns that need to be addressed.

The Department of Homeland Security's strategy is thus based on its performance of a security *screening* of relevant cargo shipment data for 100% of all containerized cargo shipments before vessel loading, and subsequent *inspections* of 100% of those containers that raise security issues after initial screening. Today, we understand that CBP inspects roughly 5.5-6% of all inbound containers (roughly 600,000 containers per

year), using either X-ray or gamma ray technology (or both) or by physical devanning of the cargo.

We all have a strong interest in the government performing as effective a security screening as possible before vessel loading. Experience also shows that substantial disruptions to commerce can be avoided if security questions relating to a cargo shipment have been addressed prior to a vessel being loaded. Not only is credible advance cargo security screening necessary to the effort to try to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or incident recovery strategy.

Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to CBP for each shipment for the before-vessel-loading security screening is the ocean carrier's bill of lading/manifest data filed under the 24 Hour Rule. This was a good start, but carriers' manifest data has limitations.

Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities.[3] *Currently, there is no data that is required to be filed into ATS by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading security screening process.* This occurs, even though these parties possess shipment data that government officials believe would have security risk assessment relevance that is not available in the carriers' manifest filings, and notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted "prior to loading in a foreign port".[4] Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until after the cargo shipment is in the United States, often at its inland destination – too late to be used for security screening purposes.

In September 2004, the COAC Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide CBP with the following data elements before vessel loading:

1. Better cargo description (carriers' manifest data is not always specific or precise)
2. Party that is selling the goods to the importer
3. Party that is purchasing the goods
4. Point of origin of the goods
5. Country from which the goods are exported
6. Ultimate consignee
7. Exporter representative
8. Name of broker (would seem relevant for security check.), and
9. Origin of container shipment – the name and address of the business where the container was stuffed, which is often not available from an ocean carrier's bill of lading.

---

[3] *See also,* "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection", General Accounting Office Report and Testimony. March 31, 2004 (GAO-04-557T).

[4] 46 U.S.C section 70116(b)(1). Section 343(a) of the Trade Act also requires that cargo information be provided by the party with the most direct knowledge of the information.

The Council agrees with this recommendation. The government's strategy today is to inspect containerized cargo on a risk-assessment basis. Accordingly, the government should improve the cargo shipment data it currently uses for its risk assessment. An ocean carrier's bill of lading by itself is not sufficient for cargo security screening. Earlier filing of these shipment data elements would improve CBP's cargo security screening capabilities.

If a risk assessment strategy is to remain the core of the government's cargo security system, the government needs to decide what additional advance cargo shipment information it needs to do the job well. It may include the data elements recommended above, or it may include additional desired data elements beyond that list. While this is not a simple task, it is important that progress be made on deciding what additional data should be obtained for this purpose, and it is important that the cargo interests, and not just carriers, be required to provide the relevant data in time to do the advance security screening before vessel loading in the foreign port.

b. Container Security Initiative

No nation by itself can secure or protect international trade. International cooperation is essential. For ships and port facilities, the International Maritime Organization (IMO), a U.N. regulatory agency with international requirement setting authority, has responded to U.S. leadership and created the International Ship and Port Security Code (ISPS). These IMO rules are internationally applicable and are strictly enforced by the U.S. Coast Guard. There is no comparable international regulatory institution with rule writing authority for international supply chain security. For a variety of reasons, the World Customs Organization (WCO) has not acquired such authority.

At the WCO, CBP continues to work with other governments on a supply chain security framework that can be used by all trading nations. This framework may be useful, but remains at a fairly high level and will be implemented on a voluntary basis by interested governments. Consequently, U.S. and foreign customs authorities must also create a network of bilateral cooperative relationships to share information and to enhance trade security. This is the Container Security Initiative. The Council fully supports this program and the strategy behind it.

Today, 73.5% of U.S. containerized imports passes through 44 operational CSI ports, with further program growth expected. CBP hopes to expand the CSI program to 55 ports, which could cover roughly 85% of U.S containerized imports.

A listing of operational CSI ports follows:

Port Name	TEUs in 2005 (in thousands) US Imports
Yantian (Shenzhen)	2,342.38
Hong Kong	1,866.14
Shanghai	1,696.41
Kaohsiung	1,154.69
Busan	1,121.67
Singapore	534.56
Rotterdam	457.32
Bremerhaven	432.68
Antwerp	317.80
Tokyo	288.77
Nagoya	187.92
Laem Chabang	178.38
Cortes	172.8
Le Spezia	158.42
Hamburg	158.41
Santos	155.70
Salalah (Oman)	129.60
Kobe	129.50
Genoa	122.87
Yokohama	122.74
Le Havre	120.83
Colombo	114.30
Gioia Tauro	96.14
Livorno (Leghorn)	96.02
Felixstowe	73.70
Algeciras	60.35
Buenos Aires	54.88
Liverpool	43.42
Tanjung Pelepas	43.25
Durban	42.26
Port Kelang	40.42
Thamesport	33.36
Naples	33.19
Southampton	32.35
Lisbon	22.90
Halifax	22.86
Gothenburg	19.13
Piraeus	10.18
Vancouver	8.99
Tilbury	2.92
Dubai	0.98
Marseille	0.69
Montreal	0.17
Zeebrugge	0.04
Total CSI Ports	*12,702.09*
Non-CSI Ports	*4,588.26*
Total All Ports	*17,290.35*

c. C-TPAT

Customs' Trade Partnership Against Terrorism (C-TPAT) is an initiative intended to increase supply chain security through voluntary, non-regulatory agreements with various industry sectors. Its primary focus is on the participation of U.S. importers, who are in turn urged to have their suppliers implement security measures all the way down their supply chains to the origin of the goods. This approach has an obvious attraction in the fact that the importer's suppliers in foreign countries are beyond the reach of U.S regulatory jurisdiction. In return for participating in the program, importers are given a benefit of reduced cargo inspection. The C-TPAT program invites participation from other parties involved in the supply chain as well, including carriers, customs brokers, freight forwarders, U.S. port facilities, and a limited application to some Mexican and Canadian manufacturers.

CBP has been working to strengthen the C-TPAT program and to increase validations of participants' performance. C-TPAT is not a regulatory program, and it is not a guarantee of security. It does, however, provide for a creative partnership approach between government and industry as one element of a multi-layered strategy to improve security. It clearly has value, even though it can't be easily measured or quantified; and, because its principal purpose is to try to affect the conduct of parties outside U.S. regulatory jurisdiction, it has a reach that regulations alone could not have.

Many maritime and supply chain security issues can be, should be, and are addressed through regulatory requirements, not C-TPAT. For example, vessel security plans and port security plans are regulated by Coast Guard regulations implementing the ISPS Code and MTSA. The data that must be filed with CBP to facilitate cargo security screening must be addressed through uniformly applied regulations. Seafarer credentials and the Transportation Worker Identification Card must be addressed through uniformly applied requirements.

C-TPAT, however, is a program that can try to address matters that are not or cannot be addressed by regulations, such as supply chain enhancements beyond U.S. regulatory jurisdiction, or matters that aren't covered by regulations.

Committee Question #2: The private sector perspective on foreign ownership of U.S. terminals

Stevedoring and marine terminal operations are a service industry that is open to foreign investment. Billions of dollars of foreign investment has been made in the U.S. over recent years in this sector, and that investment has contributed substantially to a transportation infrastructure that is critical to moving America's commerce efficiently and reliably. The investment has come from Japanese, South Korean, Danish, British, Chinese, French, Taiwanese, and Singaporean businesses, just as American companies

have been allowed to invest in marine terminal and stevedoring businesses in foreign countries.

The substantial majority of American containerized commerce is handled in U.S. ports by marine terminal operators that are subsidiaries or affiliates of foreign enterprises, usually the container shipping lines themselves. This is an international, highly competitive industry, providing hundreds of thousands of American jobs. The United States depends on it, and it in turn has served the needs of American commerce well, adding capacity and service as the needs of American exporters and importers have grown.

An important element of the U.S. government's position in international trade negotiations for many years, under both Democrat and Republican administrations, has been the importance of securing the ability of international investment to flow into various international service industries. It is a principle of substantial importance to many sectors of the American economy. There are many billions of dollars of American service industry investments around the world, including banking, insurance, food service, accounting, construction, energy, engineering, etc.

U.S. marine terminal facilities, whether operated by U.S. or non-U.S. owned companies, must and do comply with all the government's applicable security requirements. There is no evidence that terminal facilities' operations conducted by foreign controlled companies are any less secure, or in any way less compliant with security regulations, or in any way less cooperative with U.S. government security authorities than U.S. controlled companies. In fact, these companies work closely and cooperatively with the Coast Guard, Customs and Border Protection, the U.S. military, and other U.S. law enforcement agencies.

This is an international industry and has been for many years. Less than 3% of American international maritime commerce is transported on U.S.-*flag* ships, and foreign owned carriers are responsible for the capital investment in most of those ships. American *owned* liner shipping companies transport roughly 5% of the trade, and their vessels are largely foreign flag.

The leading American liner shipping companies, such as Sea-Land, APL, and Lykes, were sold by their U.S. owners years ago to foreign companies, and neither the Executive Branch nor an informed Congress did anything to protest or stop this change. Foreign ownership of shipping companies and U.S. marine terminal operating companies has been part of our nation's economic make-up for years. We live in a global economy and society where it is simply a fact that most of this important component of the nation's "critical infrastructure"[5] is owned and operated by foreign companies. One might wish

[5] The liner shipping industry and marine terminal operators logically fall within the most commonly used definitions of "critical infrastructure". *See, e.g.*, the National Infrastructure Protection Plan definition: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, networks or functions would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The

American companies were dominant industry actors, but they aren't. Further, U.S. financial markets have demonstrated little enthusiasm for international liner shipping due to its high capital investment requirements, cyclicality, and intense competition, as well as the fact that other nations' tax laws are more favorable to shipping.

The U.S. has been well served by the investment capital these foreign companies have made and continue to make in serving U.S. commerce.[6] The United States' economy and U.S. importers and exporters would be significantly harmed by policies that discourage or prevent this foreign investment. This is particularly true now with trade volumes pressing U.S. transportation infrastructure's capacity, and with ports, state governments, and the federal government all searching for additional investment capital to meet the nation's maritime transportation infrastructure needs and to keep American commerce competitive in the global market.

This nation is not at risk from foreign capital being invested in it, but it would be at risk if it were to discourage continued foreign investment in the maritime industry serving its needs.

There is another aspect to the recent Congressional interest in foreign ownership of marine terminal operators that has been myopic. In addition to the Dubai Ports World-P&O Ports transaction being mischaracterized as a purchase of U.S. ports – which it was not, and in addition to the fact that no facts were provided that showed DPW to be a security risk as a terminal operator – and in fact Dubai was shown to be an important ally and supporter of U.S. efforts in the Middle East and one which is trusted by the U.S. military to service its vessels and cargo, the entire controversy ignored the fact that, even with the six U.S. marine terminals being spun off from this purchase, DPW will be the third largest marine terminal operator in the world, and will be loading cargo onto vessels destined for the United States from its facilities in Australia, Europe, Asia and the Caribbean every day.

Wouldn't it make sense for the U.S. security strategy to try to include companies like DPW as partners of the government's efforts to secure international commerce? DPW is a knowledgeable and professional actor, both globally and in a particularly relevant part of the world. Instead, the Congress just told the third largest terminal operator in the world that it did not trust them, when the facts presented did not justify such a judgment of the company. The unfortunate treatment of this transaction should be kept confined to the narrowest possible application.

---

liner shipping industry transports roughly 11 million containers of imported goods per year to American importers and consumers, 7 million containers of exported goods from American businesses, and important government and military cargoes. The value of this goods movement is over $1.5 billion per day, and these supply chains connect the American economy to the rest of the world. The industry that is responsible for this transportation service is critical infrastructure.

[6] The hundreds of millions of dollars presently being invested in Portsmouth, Virginia by Maersk, in Mobile, Alabama by Maersk and CMA-CGM, and in Jacksonville, Florida by MOL are just three examples of this ongoing commitment to the construction of improved U.S. transportation infrastructure.

The international shipping industry and America's foreign commerce are global enterprises. Devising and implementing effective maritime security enhancements requires the participation and effort of many governments and many foreign owned and operated business enterprises. The U.S. government does not have the capability or the jurisdiction to do this by itself. It needs the cooperation and assistance of foreign governments and foreign owned businesses. The Coast Guard and Customs and Border Protection fully recognize this and are working to build and enhance global security strategies. Protectionism and unfounded criticism of foreign owned enterprises will impair those efforts and will impair security enhancement efforts.

Committee Question #3: The possible impact of terrorists smuggling a Weapon of Mass Destruction via a maritime container on global trade

The shipping industry does not know if terrorists have weapons of mass destruction, or, if they did, the likelihood that a maritime container would be used as a conduit for the transportation or delivery of such a weapon. Terrorists generally do not surrender operational control of their means of delivering an attack, and they would have to successfully evade multiple layers of security measures to succeed.

As I noted earlier, the Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability. The impact of such a possible event would be so obviously substantial, however, that there is no choice but to try to design, implement, and constantly enhance a security regime that is effective and still facilitates the efficient flow of commerce.

Committee Questions # 4 and 5: The use of radiation detection equipment and its impact on the flow of commerce, and the Hong Kong container screening concept (Integrated Container Inspection System (ICIS))

Container inspection technologies, including non-intrusive inspection (NII) equipment and radiation screening equipment, clearly have an important role in increasing both the efficiency of inspecting containerized cargo shipments and the number of containers that can be inspected. Container inspection technology, particularly NII equipment, is of substantial interest because, unlike so many other technologies, it helps address the container security question of paramount importance, namely: "What's in the box?"

Container inspection equipment is being deployed at U.S. and foreign ports.

At U.S ports, CBP has reportedly deployed 170 large scale non-intrusive inspection devices. NII inspection equipment allows Customs authorities to have a visual image of a container's contents, is a relatively easy way to review a container's contents in contrast to physically devanning the cargo, and is usually adequate for inspecting a container considered to be of security interest.

The CBP strategy is to inspect 100% of the containers that raise security questions, plus some random inspections. We understand that this comprises about 5.5% of all containers, which would be roughly 600,000 containers a year. These containers are generally subject to delays of 1-3 days in the U.S. port in order to perform the inspection, and the average cost of these inspections appears to range between $100 and $125 per container.

CBP is also deploying radiation scanning equipment at all major U.S container ports. CBP has reportedly deployed 190 radiation portal monitors at seaports to date, allowing it to scan 44 percent of arriving international cargo containers. CBP reports that this percentage will continue to grow through the remainder of this year and 2007, allowing CBP by December 2007 reportedly to scan almost all inbound cargo. The Subcommittee may wish to satisfy itself that this CBP radiation scanning plan is on schedule. CBP also has the ability to use portable devices to detect the presence of radiation, and CBP has issued over 12,000 hand-held devices to its officers with more on the way.

Radiation scanning of containers when performed at the marine terminal gate does not generally delay commerce. Deploying the technology inside terminals to also cover containers moving by on-dock rail shipment has proved more challenging.

CBP and the Department of Energy are also working with foreign ports to install NII and radiation scanning technology abroad as well. Availability of such technology is one of the criteria that a foreign port must meet to become a CSI port, for example.

The "ICIS concept" envisions the installation and operation of radiation and NII inspection equipment by marine terminal operators at foreign ports of loading, the capturing of the NII and radiation scanning images of all containers before vessel loading, the sharing and transmittal of those images to Customs authorities, and the analysis and operational use of those images in the before-vessel-loading security screening process.

This is a concept that has many potential attractions and benefits. It holds the promise of providing the ability to conduct pre-vessel loading inspections of containers entering a port facility without significant delay to commerce, and facilitating the implementation of a more effective supply chain security strategy. Such capability could enable the government to "flex" its security screening capabilities, to inspect more containers, even from a remote location, and to inspect more containers before vessel loading, rather than waiting until they arrive in the United States discharge port.

That latter point is an important one. The current U.S. container security strategy, which the Council completely supports, is to perform container security screening *before* vessel loading in the foreign port. Today, however, most container inspection and radiation screening is performed in the U.S. port of discharge. The ICIS concept would allow for much better alignment between the strategy of screening cargo containers for security risks before vessel loading and the actual capability to perform any desired inspections of such containers before vessel loading.

CBP and DHS officials are presently reviewing this technology and the pilot application of radiation-NII inspection technology to containers entering two Hong Kong port facilities. The technology is conceptually very attractive, but a real world evaluation of the technology, its effect on operations, and its integration into and use by the government is clearly needed. The following issues will have to be addressed in assessing this concept:

1. *Does the technology provide satisfactory quality and technical results?*

This is an issue requiring expert analysis that is beyond the Council's competence. We understand, however, that the preliminary review indicates that both the NII and radiation scanning products are satisfactory from a technical and quality perspective. At the same time, we note that container inspection technology will have to meet defined standards and will not remain static but be constantly refined and improved with time. We also note that there must be multiple, competitive suppliers of the inspection equipment.

2. *Is the U.S. government willing to partner and work with foreign owned and operated marine terminal operators, or will it reject them as untrustworthy?*

The "ICIS concept", as presently articulated, envisions foreign terminal operators installing and operating this inspection equipment. The recent DPW affair has clearly raised the question of whether Congress is willing to accept such a role for these companies. Will Congress accept DPW and other foreign owned terminal operators in such a role? If not, the concept as presently defined would not appear viable.[7]

3. *What is the incentive/reason that will cause marine terminal operators to install and operate such equipment?*

Assuming the U.S. government would tell terminal operators around the world that they would like them to undertake this role, its implementation would require

[7] As we understand the "ICIS concept", foreign governments' approval would be needed for the installation of the system and the operating protocols to support it, but it is not envisioned that foreign governments would be the parties purchasing and operating the equipment. An international agreement amongst trading nations for Customs authorities to purchase, install and operate such equipment on a close to universal scale is conceivable, but is not what we understand the present concept to involve.

these terminal operators to incur significant costs. We do not presently understand the "ICIS concept" to involve the U.S. government funding the purchase, installation and operation of the equipment. A commercial, profit motive of terminal operators' charging $X per container may be sufficient for them to participate in this concept, but the terminal operators are also likely to want to know: whether there are other incentives or reasons to install and operate the equipment; whether the concept if implemented has negative competitive consequences vis-à-vis terminal operators that do not install and operate such equipment; system costs, including how often the government might change the standards of the equipment it would like to see used; and, what kind of operational implications the installation and use of the equipment and system would have on their terminals, including how anomalies resulting from the equipment readings will be resolved.

4. *How is the data transmitted to Customs and Border Protection, and what are the protocols governing what CBP would be expected to do with it?*

The data files generated for millions of containers per year would not be insignificant, and practical technical data issues about the transmittal, storage, and retrieval of this data need to be understood. Are all images transmitted to CBP? Are all the images or readings that meet some particular criteria, such as a particular radiation reading, be transmitted to CBP? Does the terminal operator hold the images and provide only those requested by CBP? How many other governments will ask the terminal operator for the files?

Scanning luggage for airport security involves a review of an object containing several cubic feet of space. A standard 40 foot container contains over 2,700 cubic feet. We understand a trained CBP expert takes four to six minutes to review these images, and this must be done in conjunction with a review of the bill of lading and other shipping documents. Is image analysis software of reliable quality presently available to CBP to help with the task?

We understand the "ICIS concept" to be one to facilitate CBP inspection of all containers CBP has a question about before vessel loading, not that CBP would be expected to review all the images. Does Congress agree with this understanding?

Finally, CBP must be able to properly perform its risk assessment review of all such images of containers of interest, must be able to inform the carrier of any reason why the container should not be loaded consistent with the present 24 Hour Rule Strategy of completing cargo risk assessment *before* vessel loading, and must have agreed protocols in place with local authorities for the resolution of any security questions that arise. Suggestions that implementation issues in the foreign port of loading don't have to be addressed or that the analytical process and screening decision-making can be performed after the vessel is loaded with the cargo and is sailing for the U.S. are unacceptable from a security, a commercial, and an operating perspective.

5. *What are the protocols for what is to be done when the equipment identifies an anomaly that warrants security review?*

The current Hong Kong pilot project appears to be establishing that technology exists to capture NII images and radiation scans of containers entering a marine terminal via a road, of adequate quality, without unduly slowing down commerce. This is important. But to be useful, the technology must be integrated into an operating system that involves data transmittal, government reviews and approvals, and agreed operational protocols for what is done when the technology detects an anomaly. That remains to be done. Marine terminal operators are not interested or trained to perform the security screening of the NII images or radiation readings themselves, nor would they be likely to want to accept the potential liability for such a responsibility.

Numerous nuisance alarms are certain to occur on a regular basis, and there will need to be clear protocols for how such situations will be addressed and resolved in the foreign ports, and by whom. Tile, marble, porcelain products, kitty litter, broccoli, bananas, and other products can all set off the radiation sensor alarms, even though the cargo may be benign. Understanding how these situations would be resolved and by whom is essential. Clearly the involvement and approval of the foreign governments where the port facilities are located will be needed.

Other issues need to be understood and addressed, including how such technology might be applied to transshipped cargo, and at ports like Singapore and Rotterdam where a high percentage of the cargo does not enter the marine terminal by road through a terminal gate, but rather by barge or vessel.

6. *Does the "ICIS concept" include application to U.S. ports and U.S. export cargo? Would the U.S. agree to foreign governments' requests for reciprocity at U.S. ports?*

The Council strongly both supports the efforts of DHS and CBP to establish a priority analysis and review of this "ICIS concept" and its application and this Subcommittee's interest in the issue. The above questions are not intended to detract from the idea, but only to illustrate that the concept's application and implementation involve a number of significant issues. We are hopeful that they can be addressed satisfactorily, but the concept's implementation will take some time.

Question #6: Potential areas for improvement and recommendations for CSI, C-TPAT and global supply chain security

The maritime security challenge is to build on the fundamentally sound strategic framework that DHS has developed and to continue to make improvements on what has been started. Specifically, we believe that priority DHS consideration should be given to:

1. Improving the cargo shipment data collected and analyzed by CBP's National Targeting Center before vessel loading. If cargo risk assessment is to be a cornerstone of DHS policy -- which we believe is a correct approach, and cargo security screening is to be performed before the cargo is loaded onto a ship destined for the U.S. -- which we also believe is a correct approach, it should be using more complete cargo shipment data to perform the risk assessment than only the ocean carriers' bills of lading;

2. Continue expanding international cooperation through the Container Security Initiative network;

3. Continuing to improve and strengthen the C-TPAT program. CBP's expanded program validation efforts are an important part of this effort;

4. Promulgating regulations to implement the MTSA mandate of maritime Transportation Worker Identification Cards for U.S. port workers; and

5. Undertaking a priority examination of the merits and feasibility of widespread application of ICIS-type container inspection and radiation screening equipment and the interface and use of such equipment by Customs authorities.

Summary

When addressing the issue of international maritime security, we find ourselves dealing with the consequences of two of the more profound dynamics affecting the world today. One is the internationalization of the world economy, the remarkable growth of world trade, and the U.S. economy's appetite for imports – a demand that fills our ships, our ports, and our inland transportation infrastructure, a demand that produced more than 11 million U.S. import containers in 2005, and will produce roughly 12 million this year, and a demand that will increasingly test our ability to move America's commerce as efficiently as we have in the past.

The other dynamic is the threat to our way of life from terrorists and the challenge of addressing the vulnerabilities that exist in the free flow of international trade, even when the specific risk is elusive or impossible to identify.

Finding the correct, reasonable balance between prudent security measures and overreacting in a way that impairs commerce is a tough challenge.

Foreign equity in the international maritime transportation business is not the security challenge. It has been and continues to be a major, long-standing and positive contributor to an infrastructure that is essential to the American economy and to U.S. national security, and its interest in ensuring the safety and security of maritime commerce is very strong. After all, without a reliable, secure and efficient maritime transportation system, these companies' businesses are in jeopardy.

Mr. Chairman, the World Shipping Council and its member companies believe that there is no task more important than helping the government develop effective maritime and cargo security initiatives that do not unduly impair the flow of commerce. We are pleased to offer the Committee our views and assistance in this effort.

"A Global Terminal Operator's Perspective on Partnering with the U.S. Government on efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD"

Written Testimony before

a hearing of the

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

on

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

by

GARY GILBERT
Senior Vice President
Hutchison Port Holdings

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

10:00 a.m.
March 30, 2006

"A Global Terminal Operator's Perspective on Partnering with the U.S. Government on efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD"

by
Gary Gilbert
Senior Vice President
Hutchison Port Holdings

Chairman Coleman, Senator Levin, and distinguished members of the Permanent Subcommittee on Investigations. I am honored to appear before you this morning, to offer an industry perspective on the vital issue of confronting the risk of nuclear smuggling and supply chain security. Mr. Chairman, on behalf of Mr. John Meredith, Group Managing Director of Hutchison Port Holdings I want to thank you for the leadership you have been providing on this critical issue. We were pleased to have been afforded the chance to host you at our flagship facility in Hong Kong in December 2005 and earlier to have hosted Ray Shepherd and Brian White of your staff in August 2005. We have a long ways to go until our maritime industry is secure and I am grateful for the opportunities to offer some recommendations to advance this critical agenda.

As an introduction, I am a US born citizen and a graduate of the US Merchant Marine Academy. I have served as a ships officer on merchant and US Naval vessels including ammunition ships in the Viet Nam conflict. During a nearly 40-year career in the maritime industry I have served in the Middle East and held vice president positions in the Asia and Latin America for the former US carrier Sea Land Service. Additionally I was president and CEO of FedEx Logistics and presently serve as Senior Vice President of Hutchison Port Holdings (HPH).

HPH has been in the maritime business for 139 years originating the first registered company in Hong Kong in 1866, the Whampoa Dock Company. One of its original directors went on to form the bank HSBC. HPH is the global leader in container terminal operations handling 51.8 million containers in 2005. In 2005, American businesses imported roughly 11 million loaded containers in to the United States; approximately 40% of those containers had either been loaded at or transshipped through a HPH facility. HPH operations are spread globally over 42 locations and 20 countries.

To date, HPH operates no ports within the United States. Given that fact, you might wonder, why would our company be interested in partnering with the U.S. government on the maritime security agenda? There are two explanations for this. First, we shared the sense of shock and outrage that all Americans felt on September 11th and realized that the world had changed on that fateful day. My CEO John Meredith contacted the U.S. Consul General in Hong Kong the day after the attacks and offered any assistance that our global company could provide to manage and respond to this threat. Second, as the world's largest marine terminal operator, we know that we may be just a single terrorist incident away from having our system fail on a global scale.

To a large extent, the modern global logistics system is a result of a revolution in transportation that has gone unobserved by most Americans. The fact that up to 5000 containers loaded with a maximum of 32 tons of cargo, routinely transit the Atlantic and Pacific Oceans at the average cost of $2000, arrive on set schedules 365 days a year, has transformed the way the global economy works. To a large extent the ability of U.S. and other companies to construct global supply chains while maintaining small inventories is a result of the intermodal container that this year celebrates its 50th anniversary. As the world's largest marine terminal operator, we essentially support the conveyor belt for a growing volume of global trade that has effectively become a moving warehouse for much of America's manufacturing and retailing sectors.

My career in this industry has spanned much of this revolution that Americans take for granted. I have witnessed first hand the fruits of hundreds of billions of dollars of investment to construct an intermodal transportation system that is efficient, reliable, and low cost for its users. As a Chairman of the Corporate Security Committee for HPH, I also know that the system is vulnerable to being exploited or targeted by terrorists. Further, should such an attack lead the United States to close its ports for even a short period of time, the consequences for my industry and those who rely upon it would be devastating.

The potential for the cargo container to be exploited for an act of terror was borne out two years ago in Israel in a sparsely reported event that took place just three days after the train bombings in Madrid. On March 14, 2004, two Palestinian suicide bombers were intercepted before they reached their intended targets of several fuel and chemical storage tanks in the Port of Ashdod. The Palestinian militants killed themselves along with ten Israelis, and wounding 18 others. They reportedly evaded the security at the port facility's gate by being smuggled from Gaza in a container outfitted with a secret compartment and an arms cache. What was chilling about this incident is that it represented the first major incident where terrorists both exploited a container to get to their target and that their target of choice was a port facility.

To understand why our industry is so vulnerable to disruption, you need only to visit our flagship facility, Hongkong International Terminal, as you have recently done Mr. Chairman. Situated in the Kwai Chung container port area of Hong Kong, our 12 berths plus two more operated as a joint venture with COSCO Pacific Limited handles a combined throughput of 7.452 million TEUs. To support that kind of throughput, the facility operates 24 hours a day, 7 days a week, and 365 days a year. Typically 3-4 gantry cranes are assigned to each ship tying up at our 14 berths with an average of 35 container moves per crane per hour. Each day upwards of 10,000 trucks drive through the gates of our terminals. If we had to stop our operations for 30-minutes, we would create traffic gridlock in the Kwai Chung area. If the delay was for 2 hours, the trucks would back up to Hong Kong's border with mainland China. A 96-hour closure for a typhoon would strand tens of thousands of trucks backing them up for upwards of 100 miles into China.

But our Hong Kong terminal as well as our other 41 terminals around the world can be serious effected by closures elsewhere in the system. Our industry got a flavor of that in October 2002 when a labor dispute on the West Coast of the United States led to a 10-day closure of the port. According to Robert Parry, president of the Federal Reserve Bank of San Francisco, the estimated cost to the U.S. economy was $1 billion dollars a day during the first five days of the shutdown, rising to $2 billion dollars a day thereafter. Major retailers like Target became deeply concerned that their merchandise might not reach their store shelves in time for holiday shopping—their most important time of the year. Well over 100 large container ships were stranded at anchor outside of Los Angeles harbor causing backups and delays in the maritime transportation system around the world. Since that event, the volume of Pacific-bound container traffic has only continued to grow. As a result the consequences of a 10-day shutdown of the West Coast would be even more severe today.

In short, our industry knows that it is just a question of time before terrorists with potentially more destructive weapons will breach the security measures that have been put in place to protect the ports, the ships, and the millions of intermodal containers that link our clients to their customers. We expect that a breach involving a "dirty bomb," will lead the United States and other states to raise the port security alert system to its highest level while investigators work to sort out what happened and establish whether or not a follow-on attack is likely. Such an incident would pose an unprecedented challenge for our operations so we have a vested interest in both trying to prevent such an incident and to work closely with governmental authorities to restore the smooth operation of the system should our prevention efforts fail. This is why we have been deeply committed to support the variety of U.S. and international initiatives that have been undertaken since 9/11 to bolster port and container security. It is also why we have sought opportunities to take a leadership role in advancing innovative solutions to this very complex and high stake challenge.

Earlier this week you received testimony from Commander Stephen Flynn. HPH has known Commander Flynn since 2000. When still serving in the US Coast Guard he spent time studying container operations in our facility in Hong Kong. Commander Flynn at that time was deeply concerned about the rising threat of terrorism and the danger it posed to our industry. Sadly, we like so much of the rest of the industry, did not pay him much heed. After 9/11 we listened to Commander Flynn with new respect, realizing along with the vast majority of Americans that the world changed forever that day and we could no longer treat security as an afterthought. Prior to 9/11 we were Steve's teacher on the mechanics and economics of our industry. Now we have becoming his student, particularly in adopted the layered approach to security he has laid in his book, *America the Vulnerable*. Those layers being:

- ISPS Code
- Inspecting high-risk containers at the ports of embarkation
- Location and Tamper Evidence Monitoring
- Imaging
- Radiation Detection

A layered strategy recognizes that there is both no silver-bullet approach to security and that any one security measure travels the path of diminishing returns. That is, it gets exponentially more expensive for smaller and smaller increments of added security. As Commander Flynn has pointed out, statistically, five 60-percent measures when placed in combination will raise the overall probability of success to 99 percent. In many instances, the cost of five 60 percent measures will be less expensive than trying to bolster any one or even two measures.

HPH has put in place the first layer, the ISPS Code. We have engaged with all of our 269 carrier/customers to assure we are in full compliances with these new global standards that went into effect on 1 July 2004. We have also supported the second layer, providing support to CBP's effort to target and inspect containers that they identify as high risk at our port facilities. This has included putting into place "no load" procedures for high risk containers that CBP has so declared under the Container Security Initiative (CSI) program.

However, from the very beginning we knew that these two initiatives alone would not in our opinion solve the **Trojan Horse** problem. This is because we are both intimately familiar with the vast scope and complexity of the global supply chains and the fact that cargo often moves through some dangerous jurisdictions. As a result, we worry that CBP may be overestimating their ability to accurately assess true risk within our industry. Particularly worrisome it the extent to which CBP's relies for their primary screen, the commercially supplied ocean carrier's bill of lading/manifest data that is filed under the 24-hour rule; that is CBP requires this manifest data be furnished to them 24 hours prior to vessel loading which it examines against its risk-based rules and other intelligence it might have. CBP defines this electronic data review as "screening" 100 percent of all containers for risk. Approximate 1 percent of these containers are given a "No Load" order overseas and they then are inspected by the host government at the request of the CSI team. Presently, we understand that 1% reflects only 20 percent of all the US bound containers that CBP is actually concerned about. The remainder is inspected when they are discharged within a US port bringing the total amount of containers examined to 5 percent. The question that this should raise for this committee is wouldn't it be better to examine all the containers deemed to be at risk before they are loading on a U.S. bound ship? Better yet, since we believe that it is not possible to rule out risk for any of the 52 million containers entering HPH network of container terminals, the U.S. government and the international community should be striving to construct a *Trust but Verify* strategy for the global supply chain. This can be accomplished by working with existing programs, but by adding additional layers of security.

At HPH, we have also been hard at work trying to enhance security throughout the supply chain. Early in 2002 we worked to rapidly deploy a baseline functional capability in location and tamper evidence monitoring leveraging off the shelf/proven DOD radio frequency identification(RFID) technology using the global networks of the top three global port operators (HPH, PSA, P&O) as strategic control points in the global supply chain. In a pilot named Smart and Secure Tradelanes (SST) we collectively

moved/tracked over a thousand boxes. Key participants were Target Stores, Michelin, Hewlett Packard, Xerox and BASF along with APL, Mitsui OSK and Maersk Logistics. To enable this capability, HPH equipped its four largest terminals (Hong Kong, Rotterdam, Felixstowe and Yantian) with RFID readers and software. HPH has participated in four Operation Safe Commerce (OSC) projects. We have participated in CBP's Smart Box trials. We have been in the lead in the deployment of radiation detection equipment with UK Customs in Felixstowe, United Kingdom and deployment under the NNSA program in Rotterdam, Netherlands and Freeport, Bahamas.

At HPH we also believe that it is possible to configure our facilities to support a much a high percentage of verifications. This would come from deploying non-intrusive inspection (NII) equipment to examine containers arriving in overseas terminals loading to the US. That examination would include; a scanned picture of the containers' contents, a radioactivity exam, radio frequency identification (RFID) of the seal and a photo of the exterior of the container noting the container number. Such information would be placed into a computer file enabling it to be transmitted and examined remotely by inspectors. This data collection of verification of the contents of the container does not need to be limited to only US bound containers. The cost of deploying, maintaining, and upgrading the NII equipment would be largely borne by the private sector. The terminal operators would establish a fee to recover their costs that would range from $10-20 per container—the greater the volume of containers, the lower the surcharge. With overseas container terminals verifying the contents, all containers prior to loading this screening data would be collected for cargo moving to other jurisdictions as well, thereby enhancing the means to detect the movement of nuclear-related materials that are bound for other locations such as Iran.

This proposed high volume container screening system has been in operation for well over a year in Hong Kong sponsored by the Hong Kong Container Terminal Operators Association. It is operating within two of the busiest marine terminals in the world. Beginning in 2005, every truck entering the main gates at Hong Kong International Terminal and Modern Terminal has passed through portal screening technologies creating a database of over 1.5 million images. Key to this pilot has been the industrial engineering aspect. We have sought to deploy the system so that the entering containers are brought into the facilities at normal speed versus being required to come to rest for the scan as is the typical practice. The pilot was designed to test and confirmed that it would be possible to consistently collect NII images at speeds of up to 15 kph, 24 hours a day, without disrupting the normal traffic flow into the marine terminals. These images are the same as those that are routinely collected approximately 1 percent of containers that are targeted by DHS for inspection prior to loading. The pilot is being evaluated by DHS/CBP which has under review a sample of 20,000 container scans and radiation signatures from this pilot. We have also offered to work with CBP on identifying how current examination protocols should be adapted to tap the potential of this screening system. The technology is proven and there are several manufacturers that can provide the equipment. Important improvements in the quality of the inspections, the quantity of inspections, their accuracy, and operational speed can be expected in the next 1-3 years. Because terminal operators will be able to recover their costs by setting a fee in their

terminal tariffs, they are able to purchase off-the shelf equipment now and than upgrade once the next generation equipment becomes available.

The present focus on ports and containers is long overdue. However, we believe that the Congress and the American people need to focus on achievable goals and not become overwrought by their worst fears. There are enormous national security and economic security interests at stake should the next catastrophic terrorist attack on U.S. soil involve the global maritime transportation system and America's waterfront. The best way to address that threat is to rapidly move towards a **Trust but Verify** policy, partnering with foreign overseas terminal operators like my company that are prepared to become an industry **Coalition of the Willing** to rapidly deploy the best technology and develop the best operational practices to support this critical mission. At the end of the day, Americans must understand that the maritime transportation system they are so dependent upon is nearly entirely operated by private companies that are not headquartered in the United States. In fact the four major container terminal operators loading 80% of the containers moving around the globe are headquartered in Hong Kong, Denmark, Dubai and Singapore. DP World is one of those four companies. The others are Hutchison Port Holdings (HPH), A.P.Moller Terminals (APMT) and Port of Singapore Authority (PSA).

Mr. Chairman, I was profoundly moved by the discourse between Governor Kean and Senator Lautenberg on Tuesday as they discussed just when an issue is a priority? You could see them reliving in their minds that terrible day in September 2001. HPH had two British associates in the Twin Towers on 9/11. Ironically, John Meredith had personally sent them to New York to explore what opportunities might exist for HPH to invest in the United States. Mr. Meredith was very worried about their welfare and relieved at their survival. He saw the US airports closed as the U.S. government struggled both to understand what happened and how best to react. As the leader of the global port industry he immediately realized what the effects might have been on the global trade system should the attacks of that day involved a ship or a maritime container instead of an aircraft.

Since 9/11, our company have invested over $200 million dollars to elevate the security of worldwide facilities. At my CEO's direction we have also been actively pursuing a number of self funded pilots that we believe will support the U.S. government's efforts to secure the global supply chain. While HPH does not operate ports inside the United States, John Meredith has come to Washington D.C. every year since 9/11 to offer his support and advice and even to voluntarily commit to make our company's resources to address the issue. What is his motive for doing so even in the face of the occasional spurious attack in recent days by some in the U.S. media: John Meredith is exercising private sector leadership on something that he believes to be one of our times most urgent issues and one that deserves to be **a global priority.**

Mr. Chairman, thank you again for your leadership on this critical issue and the opportunity to address your committee and I look forward to answering any of your questions.

212

TESTIMONY OF

JOHN P. CLANCEY, CHAIRMAN, MAERSK, INC.,

BEFORE THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

COMMITTEE

UNITED STATES SENATE

MARCH 30, 2006

Mr. Chairman, my name is John Clancey, and I am Chairman of Maersk Inc. I appreciate the opportunity to appear before the Subcommittee this morning to discuss the very important issue of maritime security.

As you may know, Maersk is one of the largest liner shipping companies in the world, serving customers all over the globe. With a fleet numbering more than 500 container vessels and about 1.4 million operated containers, we provide reliable and comprehensive ocean shipping transportation. Maersk, Incorporated is the North America agent for parent company A.P. Moller-Maersk Group's liner businesses, Maersk Line and Safmarine. The A.P. Moller-Maersk Group employs more than 70,000 people in over 125 countries.

In 1943, Maersk, Inc. was established as the general agent for A.P. Moller's liner business, Maersk Line. Here in the United States, we generate employment for approximately 12,000 Americans and we have committed to significant infrastructure investments before and since September 11, 2001.

My tenure in the ocean shipping industry - with Maersk and predecessor companies - spans more than three decades during which I have had commercial, operational and management responsibilities in nearly every major tradelane and market in the world. Our business includes liner shipping, terminal operations, logistics, warehousing and supply chain operations (and other businesses) related to the global movement of freight.

Maersk has been actively involved in maritime security issues for many years. Our commitment to security is captured by the watch words for all our activities: "Constant Care." The security of our containers and the integrity of our transportation network are essential to our operations at Maersk. Marine transportation is a worldwide industry, and it is inherently intermodal -- a container that is unloaded at a U.S. seaport today can be almost anywhere in the nation tomorrow or within days.

For many years, cargo moved fluidly through our ports and facilities subject to prevailing regulations. But the events of September 11, 2001 changed the way we think about maritime security. Maersk Line and other carriers serving the United States today are more concerned than ever about security threats, for we know that terrorist elements might seize upon our transportation mode as an attack opportunity.

Mr. Chairman, in your letter of invitation, you requested that I address several specific matters in my testimony.

Let me begin by commenting on Maersk's perspective on U.S. government programs related to maritime and port security. Many Federal Government maritime security programs are successful. But neither the government nor private industry can achieve maritime security unilaterally; it requires joint efforts. Maersk participates in the Maritime Security Program (MSP), which we believe provides a cost-efficient way for U.S. interests to be guaranteed, while at the same time providing benefits to liner companies. In addition, we have entered voluntarily into a variety of U.S. government programs and pilot projects – for example, we were the first enterprise-wide transportation company to be validated by the Customs-Trade Partnership Against Terrorism (C-TPAT) Program. We support the continuation of C-TPAT, strongly believe that the program should remain voluntary and not subject to governmental rulemaking, and maintain that it should be flexible enough to permit variations in its application to participants and not impose a generic set of mandatory rules on all of them.

Maersk also participates in the Super Carrier Initiative Program, one of approximately 27 ocean carriers worldwide permitted by U.S. Customs and Border Protection (CBP) to participate at this level. We strongly support U.S. authorities performing the inspection function at foreign ports -- before any container is loaded on a vessel. We are working cooperatively with U.S. officials to achieve this desirable result.

Another area of our work with the government involves the issue of employee identification. As you know, the Maritime Transportation Security Act of 2002 (MTSA) mandated that the government develop and issue credentials (including biometric identifiers and background checks) for transportation workers seeking unescorted access to secure areas within transportation facilities. We support the concept of the Transportation Worker Identification Card (TWIC), and we will provide information to assist in improving employee identification and assist in the implementation of the TWIC program.

But we realize that it is not enough to make maritime operations within this country secure, so Maersk has intensified efforts to secure the company's international cargo network through the establishment of a comprehensive and vigorous global security policy and strategy that governs our sea and landside operations worldwide.

In short, we agree that maritime security here and abroad can be improved, and we are working cooperatively to achieve this objective, both in partnership with the government and through our own efforts. We have some concerns that governmental efforts and partnerships not be duplicative, commercially punitive or inconsistent, or add unnecessary levels of bureaucracy. Security is already a very complicated area, and additional levels of paperwork and involvement by multiple agencies will not further the overall goal of making our marine transportation system safer.

You inquired about the use of radiation detection equipment at seaports, and possible impacts from the use of such equipment. We have had success in working on this matter with CBP. For example, it was proposed originally that this equipment be located at terminal wharfs and yards, but that would have caused significant delay and disruption. Through collaborative discussions with CBP we were able to locate the devices elsewhere at the terminal in a manner that causes minimal negative effects on commercial operations but also achieves the high level of security sought by CBP. I would note that sufficient funding must be provided to enable CBP to carry out its responsibilities of foreign port inspections. Any concept of non-intrusive inspection requires that images from screening be reviewed by CBP and that terminal operators in foreign ports receive feedback from CBP. This program can work, but the CBP's databases need to be updated and designed so that images can be matched in real time with information on file with CBP. Then, in cases where further inspection is required, the additional inspection can occur immediately. If the system does not work well and efficiently, there will be significant negative impacts on the flow of goods in international commerce. For instance, in the port of Newark, NJ, over 200 radiation alerts occur daily. Most are consistent with the nature of the goods but all require further action to resolve.

A third area of inquiry relates to foreign ownership of U.S. terminals. Congressional concern regarding the Dubai Ports World/P&O Ports transaction indicates a need for a clear understanding of the role, investments and commitment that marine terminal operators are playing in global trade and, ultimately, the economic prosperity of the United States.

A marine terminal operating company typically holds a long-term lease from a public (local or state) port authority to manage a loading/unloading marine facility. It is a specialized, highly competitive, low-margin business whose tools – a dock, a crane, and a parking lot -- are in the hands of American union labor and American management personnel.

The shipping industry has always been highly globalized and highly competitive. Billions of dollars in foreign investment from Japanese, South Korean, Danish, British, Chinese, French, Taiwanese and Singaporean companies have been invested in the United States. (For example, Maersk has invested or committed more than $3 billion in U.S. port projects since September 11, 2001). Today, foreign-owned companies are running the majority of U.S. marine terminals, and there are at least three major reasons for this fact:

- Port authorities prefer large, predictable volumes that can only be guaranteed by liner shipping companies, almost all of which are foreign-owned. So liner-affiliated, foreign terminal operators are the top priority sales targets for American port authorities seeking to grow their businesses.
- Liner companies prefer handling their own landside terminal operations in order to assure service quality and control costs. Since the global liner companies serving U.S. markets are foreign-owned, their terminal operations are also foreign-owned. This has been the case for many years.
- Large terminal operators know that they must be located where the freight-flows are, if they are to serve their customers comprehensively. Since America is the largest consuming market for freight, every terminal operator wants to be represented and well-positioned in the United States.

Terminal operators operate within lease agreements typically awarded and administered by the local port authority. Port authorities and their lease-holding operators and the carrier customers they serve must (and do) comply with American and international security codes, rules and laws under the jurisdiction of the Coast Guard, the Department of Homeland Security (DHS), and other law enforcement agencies. There has been no evidence that foreign-controlled companies are any less secure, or in any way less compliant with security regulations, or in any way less cooperative with U.S. government security authorities than domestic operators. Indeed, the international shipping industry – of which terminal operations is a key component – is a committed investor, a high-quality service provider and a staunch collaborative partner with the United States in all trade and security issues.

Mr. Chairman, your letter raised the potential impacts from a terrorist element smuggling a Weapon of Mass Destruction into our nation utilizing a maritime container; obviously, this is a grave concern. We must take prudent, effective and cost-efficient means to prevent that occurrence. One very significant component of improved maritime security is the advanced filing of the vessel cargo manifest. This manifest, based on long standing regulatory and commercial standards, provides a great deal of specific, useful information on all cargo that is brought into the United States. Among other items, it identifies the declared contents of the container or the cargo carried onboard the vessel, the identity of the shipper and consignee, the port of origin, and the destination within the United States. We believe that more specific shipment information supplemental to the manifest is needed. It is the responsibility of shippers who possess this information to

provide it to Customs where confidentiality and integrity of the data can be protected. Of course, we also must be certain that the right kind of information is collected as ocean carriers do not have – nor is there a need to have – this type of information. Authorities must be sure that the shipper-collected information can be acted upon quickly, and that this process does not introduce an unreasonable amount of friction into the flow of global trade.

I mentioned earlier the potential from non-intrusive inspections or an ICIS (Integrated Container Inspection System) -type initiative. This type of protocol can be a very useful tool in the campaign to ensure maritime security but there are some concerns. First, how do we ensure participation at foreign ports? There has to be an incentive structure or bi-lateral agreements with foreign governments in order to make the inspections uniform and comprehensive. Second, proprietary information is generated by this process and confidentiality of this information must be safeguarded. Third, liner companies don't have sovereign immunity and therefore cannot be in the position of making decisions about which containers are high risk. Additionally, there are operational concerns having to do with process and speed. The bottom line, however, is that we are ready to cooperate with CBP and other relevant governmental agencies on this development once these outstanding concerns have been adequately addressed.

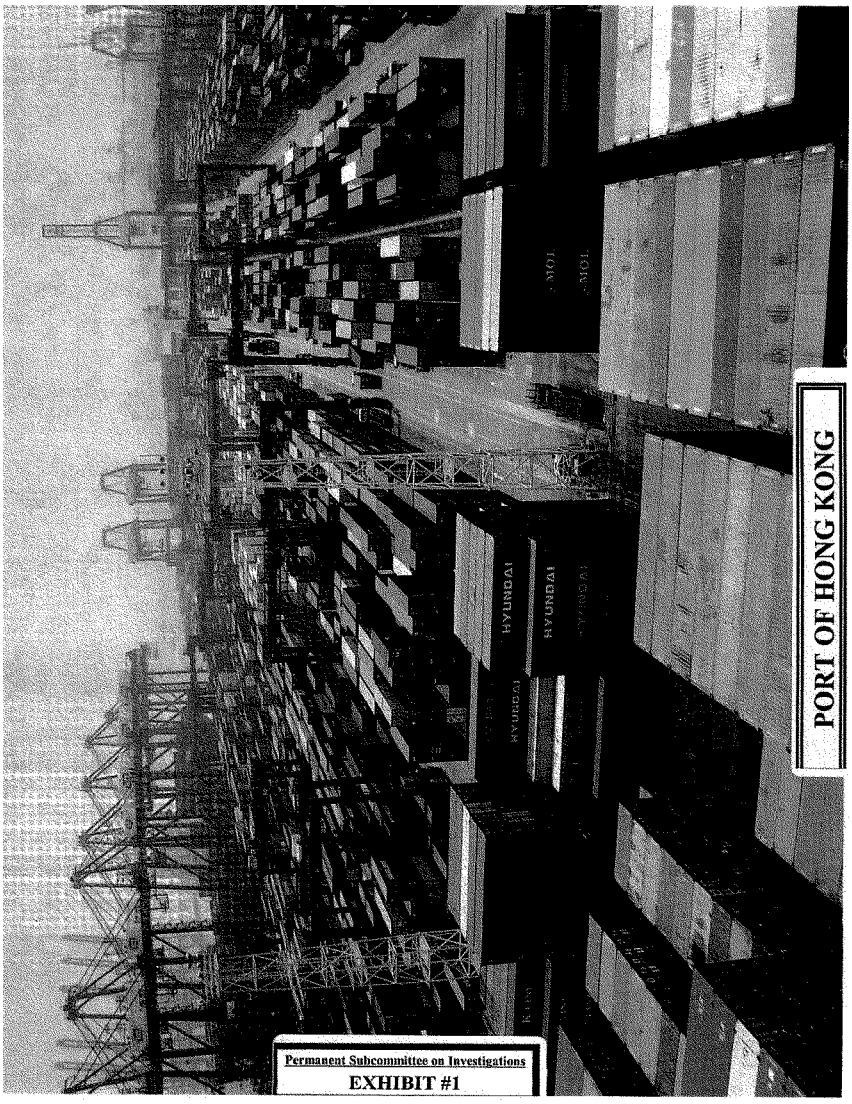
Mr. Chairman, finally you asked about specific maritime security recommendations. In general, I would encourage policymakers to evaluate potential requirements with an eye toward trade reciprocity, and their application to both imports and exports. We must anticipate whether our foreign trade partners will impose similar requirements, and whether it is feasible for U.S. interests to comply.

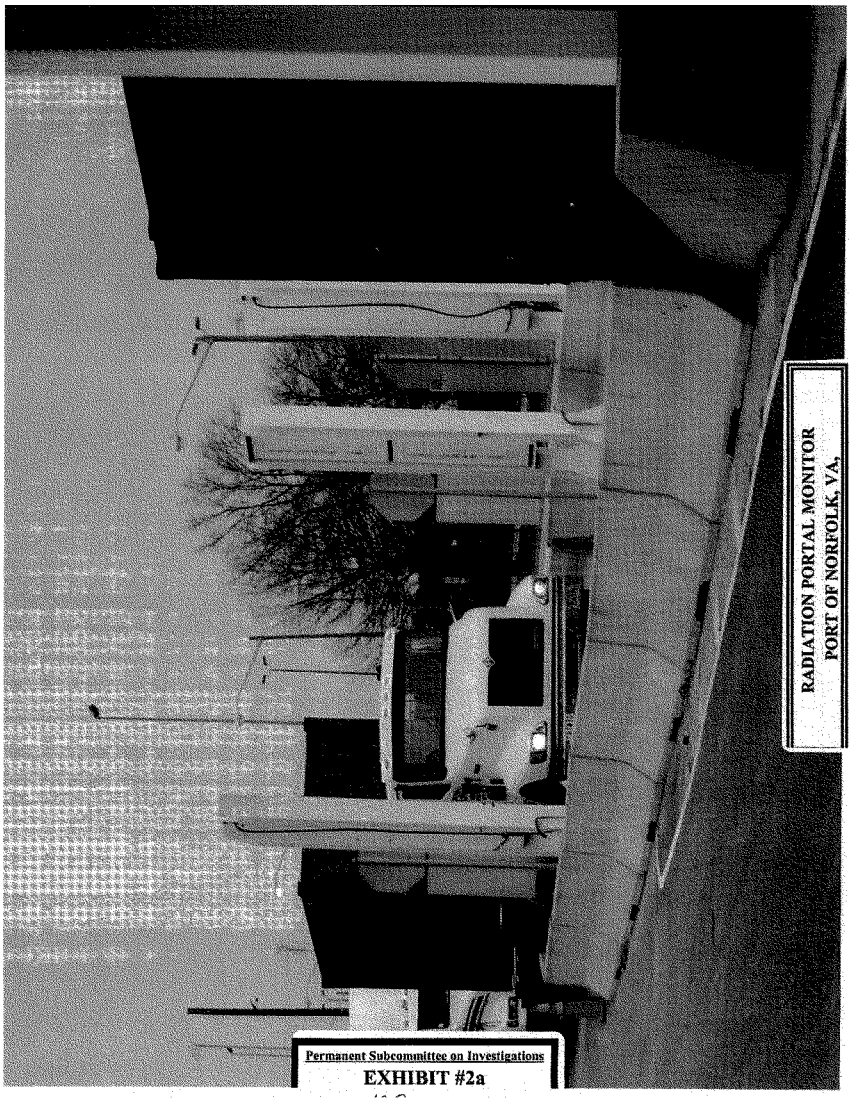
Some have proposed a kind of "trusted carrier/shipper" program whose participants would receive expedited treatment in international commercial transport. If such a program is adopted, it must provide clear, direct benefits to all participants in return for implementing high security standards. This is essential if companies are going to undertake the investment needed to become involved in the program and make the changes the program requires.

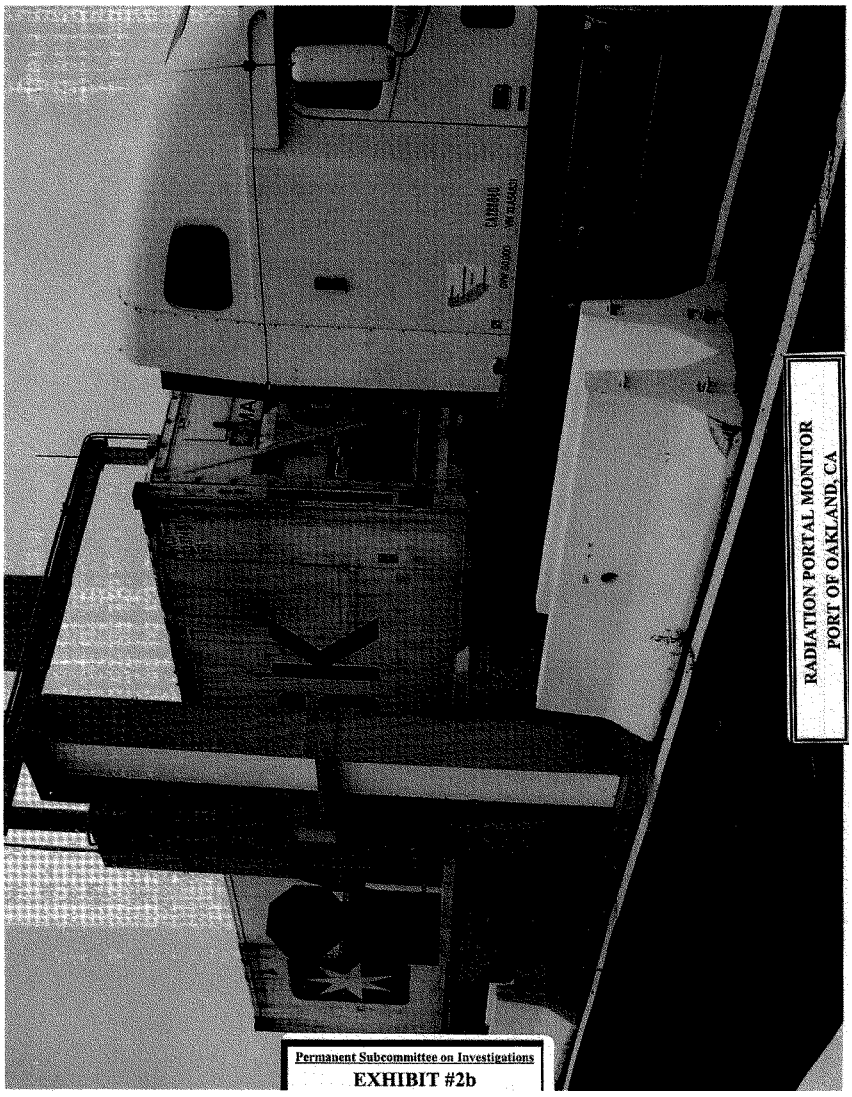
Some advocate that container security devices be required immediately. The MTSA already requires that DHS set standards for these devices, and CBP and DHS are testing devices against these standards. But as we are all aware, many of the prospective technologies out there are a long way from production reality. We are all highly interested and share a sense of urgency and will await the outcome of comprehensive testing to determine their technological feasibility before proceeding on this matter. We know that no such device currently operates at the necessary level of accuracy and reliability.

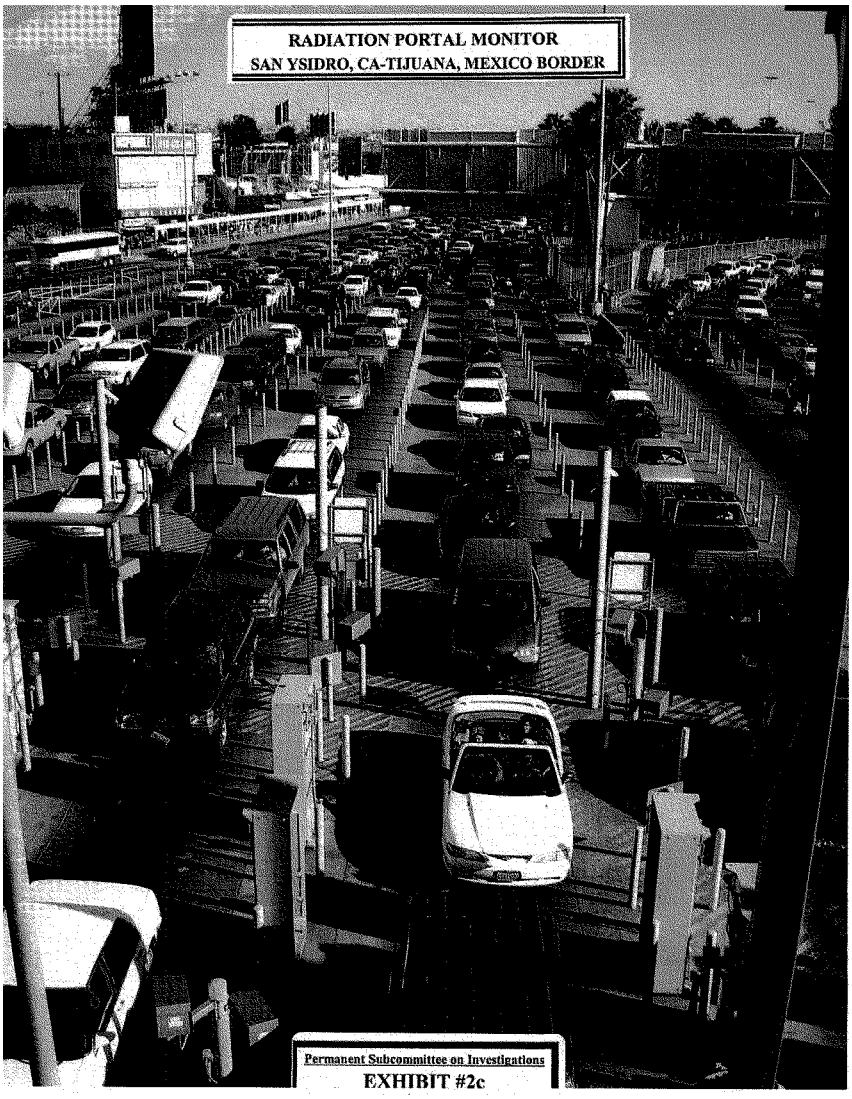
Mr. Chairman, Maersk works hard to make our operations as safe as possible. This is in the national security interests of our country, our own commercial interests, and the interests of providing a safe and secure workplace environment for our employees. "Constant Care" are our watchwords, and they form the foundation of every activity we take in this regard.

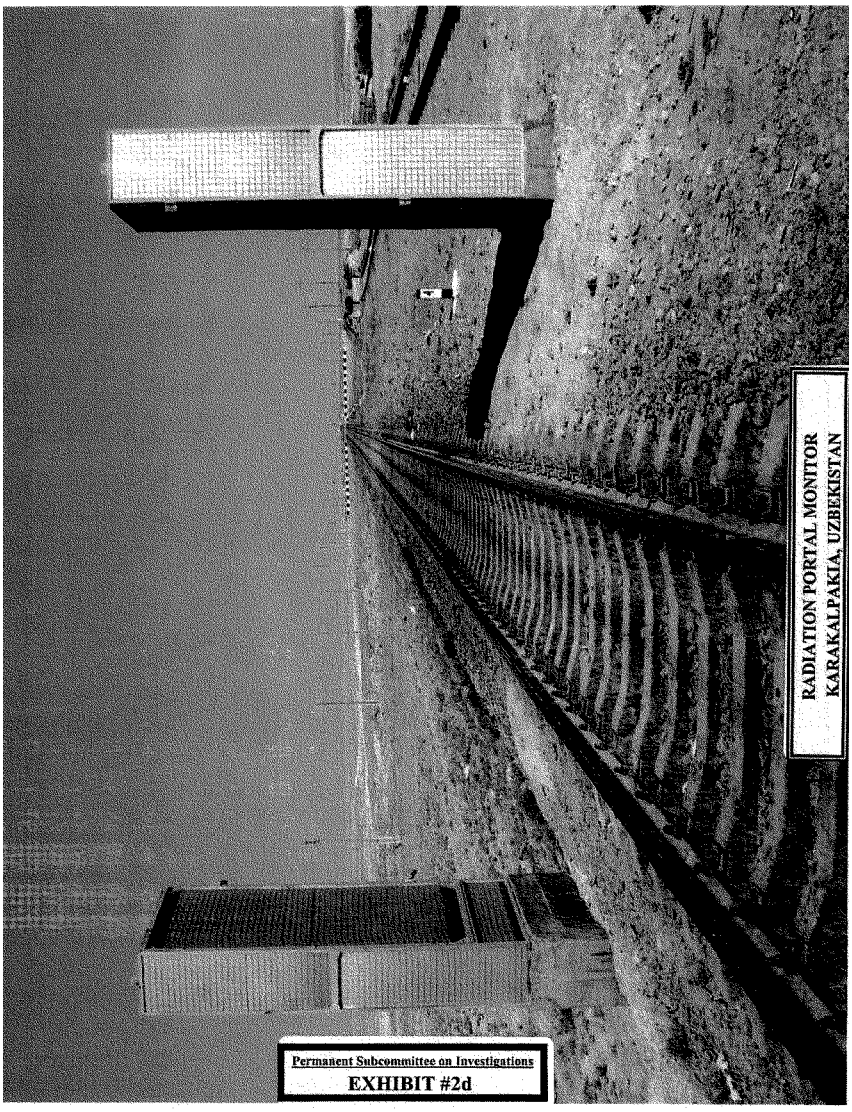
We at Maersk look forward to continuing to discuss maritime security issues with you. I am happy to attempt to answer any questions you may have, and I appreciate very much the opportunity to appear before you this morning.


PORT OF HONG KONG
Permanent Subcommittee on Investigations
EXHIBIT #1


RADIATION PORTAL MONITOR
PORT OF NORFOLK, VA.
Permanent Subcommittee on Investigations
EXHIBIT #2a


RADIATION PORTAL MONITOR
PORT OF OAKLAND, CA
Permanent Subcommittee on Investigations
EXHIBIT #2b


RADIATION PORTAL MONITOR
SAN YSIDRO, CA-TIJUANA, MEXICO BORDER
Permanent Subcommittee on Investigations
EXHIBIT #2c


RADIATION PORTAL MONITOR
KARAKALPAKIA, UZBEKISTAN
Permanent Subcommittee on Investigations
EXHIBIT #2d

United States Government Accountability Office

GAO

Report to Congressional Requesters

March 2006

COMBATING NUCLEAR SMUGGLING

Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries

GAO-06-311

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-311, a report to congressional requesters

March 2006

COMBATING NUCLEAR SMUGGLING

Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries

Why GAO Did This Study

According to the International Atomic Energy Agency, between 1993 and 2004, there were 662 confirmed cases of illicit trafficking in nuclear and radiological materials. Three U.S. agencies, the Departments of Energy (DOE), Defense (DOD), and State (State), have programs that provide radiation detection equipment and training to border security personnel in other countries. GAO examined the (1) progress U.S. programs have made in providing radiation detection equipment to foreign governments, including the current and expected costs of these programs; (2) challenges U.S. programs face in this effort; and (3) steps being taken to coordinate U.S. efforts to combat nuclear smuggling in other countries.

What GAO Recommends

GAO is making recommendations to the Secretaries of Energy and State to (1) integrate cost projections for anticorruption measures into long-term program cost estimates; (2) upgrade less sophisticated portal monitors; (3) provide maintenance for all handheld radiation detection equipment provided by U.S. programs; (4) revise the interagency strategic plan; and (5) compile, maintain, and share a master list of all U.S. radiation detection equipment assistance.

DOE and State generally agreed with our conclusions and recommendations. DOD did not provide comments on the report.

www.gao.gov/cgi-bin/getrpt?GAO-06-311.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gene Aloise at (202) 512-5841 or aloisee@gao.gov.

What GAO Found

Since fiscal year 1994, DOE, DOD, and State have provided radiation detection equipment to 36 countries as part of the overall U.S. effort to combat nuclear smuggling. Through the end of fiscal year 2005, these agencies had spent about $178 million on this assistance through seven different programs. Primary among these programs is DOE's Second Line of Defense "Core" program, which has installed equipment mostly in Russia since 1998.

U.S. efforts to install and effectively operate radiation detection equipment in other countries face a number of challenges including: corruption of some foreign border security officials, technical limitations of some radiation detection equipment, inadequate maintenance of some equipment, and the lack of supporting infrastructure at some border sites. DOE, DOD, and State officials told us they are concerned that corrupt foreign border security personnel could compromise the effectiveness of U.S.-funded radiation detection equipment by either turning off equipment or ignoring alarms. In addition, State and other agencies have installed equipment at some sites that is less effective than equipment installed by DOE. Since 2002, DOE has maintained the equipment but has only upgraded one site. As a result, these border sites are more vulnerable to nuclear smuggling than sites with more sophisticated equipment. Further, while DOE assumed responsibility for maintaining most U.S.-funded equipment, some handheld equipment provided by State and DOD has not been maintained. Lastly, many border sites are located in remote areas that often lack infrastructure essential to operate radiation detection equipment.

As the lead interagency coordinator of all U.S. radiation detection equipment assistance overseas, State has taken some steps to coordinate U.S. efforts. However, its ability to carry out its role as lead coordinator is limited by shortcomings in the strategic plan for interagency coordination. Additionally, State has not maintained an interagency master list of all U.S.-funded radiation detection equipment overseas. Without such a list, program managers at DOE, DOD, and State cannot accurately assess if equipment is operational and being used as intended; determine the equipment needs of countries where they plan to provide assistance; or detect if an agency has unknowingly supplied duplicative equipment.

DOD-Funded Radiation Portal Monitor in Uzbekistan

Source: DOD

Contents

Abbreviations

CRITr	Cooperative Radiological Instrument Transfer project
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOE	Department of Energy
DOD	Department of Defense
EXBS	Export Control and Related Border Security program
GBSLE	Georgia Border Security and Law Enforcement program
ICP	International Counterproliferation Program
IAEA	International Atomic Energy Agency
NDF	Nonproliferation and Disarmament Fund
NNSA	National Nuclear Security Administration
RIID	radioactive isotope identification device
SLD-Core	Second Line of Defense "Core" program
WMD	weapons of mass destruction
WMD-PPI	Weapons of Mass Destruction Proliferation Prevention Initiative

GAO
Accountability • Integrity • Reliability

United States Government Accountability Office
Washington, D.C. 20548

March 14, 2006

Congressional Requesters

According to the International Atomic Energy Agency, between 1993 and 2004, there were 662 confirmed cases of illicit trafficking in nuclear and radiological materials, and the number of reported cases has risen dramatically since 2002. Many of these cases involved material that could be used to produce either a nuclear weapon or a device that uses conventional explosives with radioactive material (known as a "dirty bomb," or radiological dispersal device). Especially in the aftermath of the attacks on September 11, 2001, there is heightened concern that terrorists may try to smuggle nuclear materials or a nuclear weapon into the United States. If terrorists were to accomplish this, the consequences could be devastating to our national and economic interests. In April 2004, the United Nations Security Council passed a resolution calling for every member state to put in place appropriate effective border controls and law enforcement to detect, deter, prevent, and combat the illicit trafficking and brokering in nuclear materials and other items related to weapons of mass destruction.[1]

In response to the growing concern about nuclear smuggling, three U.S. agencies, the Departments of Energy (DOE), Defense (DOD), and State (State), have programs that provide radiation detection equipment and related training to border security personnel and customs officials in other countries.[2] Initial concerns about the threat posed by nuclear smuggling were focused on nuclear materials originating in the former Soviet Union. As a result, the first major initiatives to combat nuclear smuggling concentrated on deploying radiation detection equipment at borders in countries of the former Soviet Union and in Eastern Europe. Beginning in the mid-1990s, DOD and State provided fixed radiation detection equipment, known as radiation portal monitors, and handheld radiation detection equipment to a number of countries in this region. In 1998, DOE

[1]See S.C.Res. 1540, U.N. Doc. S/RES/1540 (Apr. 28, 2004).

[2]In addition to DOE, DOD, and State's efforts to combat nuclear smuggling in other countries, the Department of Homeland Security (DHS) is installing radiation detection equipment at U.S. ports of entry. We recently reported on DHS's efforts in GAO, *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain*, GAO-06-389 (Washington, D.C.: Mar. 14, 2006).

established the Second Line of Defense "Core" (SLD-Core) program,[3] which has primarily worked to help Russia detect illicit nuclear materials trafficking by providing radiation detection equipment to the Federal Customs Service of Russia. In coordination with State, DOE, through its National Nuclear Security Administration,[4] has recently expanded its efforts in the SLD-Core program to include countries other than Russia, including installing radiation detection equipment at border sites in Greece as part of the overall U.S. effort to provide security assistance prior to the 2004 Olympic Games.[5] In addition to DOE's efforts through the SLD-Core program, six other programs—one at DOE, two at DOD, and three at State—have provided radiation detection equipment to assist foreign governments in combating nuclear smuggling. Further, State is the lead interagency coordinator of U.S. nuclear detection assistance overseas.

As agreed with your offices, this report addresses U.S. efforts to combat nuclear smuggling by examining (1) the progress U.S. programs have made in providing radiation detection equipment to foreign governments, including the current and expected costs of these programs; (2) the challenges U.S. programs face in deploying or operating radiation detection equipment in foreign countries; and (3) the steps being taken to coordinate U.S. efforts to combat nuclear smuggling in other countries. To address these objectives, we analyzed documentation on U.S. efforts to combat nuclear smuggling from DOE and its contractors, both at DOE's national laboratories and in the private sector; DOD and its contractors; State; and

[3]We originally reported on U.S. efforts to combat nuclear smuggling in 2002. For additional information, see GAO, *Nuclear Nonproliferation: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning*, GAO-02-426 (Washington, D.C.: May 16, 2002).

[4]The National Nuclear Security Administration is a separately organized agency within DOE that was created by the National Defense Authorization Act for Fiscal Year 2000, Pub. L. No. 106-65 (2000), with responsibility for the nation's nuclear weapons, nonproliferation, and naval reactors programs.

[5]Additionally, in 2003, DOE began implementing a related program, the Megaports Initiative, to focus on the threat posed by nuclear smuggling at major foreign seaports. We recently reported on this program; therefore, we will not address the Megaports Initiative in this report. For additional information, see GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports*, GAO-05-375 (Washington, D.C.: Mar. 31, 2005). Through January 2006, DOE had completed installations at four ports in Greece, the Netherlands, Sri Lanka, and the Bahamas. DOE anticipates completing an additional port in Spain in April 2006. DOE has signed agreements to begin work at ports in seven other countries (China, Honduras, Israel, Oman, the Philippines, Thailand, and the United Arab Emirates).

DHS and conducted interviews with key program officials at each of these agencies. We also visited six countries (Georgia, Greece, Macedonia, Russia, Ukraine, and Uzbekistan), where U.S. agencies have provided radiation detection equipment, to observe U.S.-funded radiation detection equipment in operation and to discuss the implementation of U.S. programs with foreign officials. In addition, we analyzed cost and budgetary information from DOE, DOD, State, and DHS; performed a data reliability assessment of this data; and interviewed knowledgeable agency officials on the reliability of the data. We determined these data were sufficiently reliable for the purposes of this report. More details on our scope and methodology can be found in appendix I. We conducted our review from April 2005 to February 2006 in accordance with generally accepted government auditing standards.

Results in Brief

Since fiscal year 1994, DOE, DOD, and State have provided radiation detection equipment to 36 countries as part of the overall U.S. effort to combat nuclear smuggling. Through the end of fiscal year 2005, these agencies had spent about $178 million on this assistance through seven different programs. Specifically, as of fiscal year 2005, DOE's SLD-Core program had completed installation of radiation portal monitors at 83 border sites in Russia, Greece, and Lithuania at a cost of about $130 million. DOE plans to install radiation detection equipment at a total of about 350 sites in 31 countries by 2012 at a total cost of about $570 million. A second DOE program has provided handheld radiation detection equipment to regulatory agencies and patrol officers in 9 countries at a cost of about $1 million. In addition to DOE's efforts, two DOD programs have spent about $22 million to provide radiation portal monitors, handheld equipment, and radiation detection training to 8 countries in the former Soviet Union and Eastern Europe. DOD plans to complete its Uzbekistan Portal Monitoring project in fiscal year 2009 at a total cost of about $54 million. Furthermore, DOD also plans to continue providing limited amounts of handheld radiation detection equipment to other countries in the future. Similarly, three Department of State programs have provided radiation detection equipment and training to 31 countries at a cost of about $25 million. However, future spending requirements for State's radiation detection assistance programs are uncertain, in part, because State's Export Control and Related Border Security program provides radiation detection equipment to foreign countries on an as needed basis as a part of its effort to increase export control enforcement in foreign countries. In coordination with DOE, this program also selectively funds more expensive radiation portal monitors to certain sites on a case-by-case

basis, such as at one site in Armenia, where State believes the imminence of a smuggling threat warranted immediate action.

U.S. efforts to provide radiation detection equipment to other countries face a number of challenges that can impact the effective operation of this equipment, including: possible corruption of border security officials in some countries, technical limitations of radiation detection equipment previously deployed by State and other agencies, inadequate maintenance of some equipment deployed by DOD and State, and the lack of infrastructure and harsh environmental conditions at some border sites.

- According to officials from several recipient countries we visited, corruption is a pervasive problem within the ranks of border security organizations. DOE, DOD, and State officials told us they are concerned that corrupt foreign border security personnel could compromise the effectiveness of U.S.-funded radiation detection equipment by either turning off equipment or ignoring alarms. To mitigate this threat, DOE and DOD plan to deploy communications links between individual border sites and national command centers so that alarm data can be simultaneously evaluated by multiple officials, thus establishing redundant layers of accountability for alarm response. In addition, DOD plans to implement a program in Uzbekistan to combat some of the underlying issues that can lead to corruption through periodic screening of border security personnel. State also conducts anticorruption training as part of its overall export control assistance to foreign countries.

- Some radiation portal monitors that State and other U.S. agencies previously installed at foreign border sites have technical limitations and can only detect gamma radiation, which makes them less effective at detecting weapons-usable nuclear material than equipment with both gamma and neutron radiation detection capabilities. Since 2002, DOE has maintained this equipment but has not upgraded any of it, with the exception of one site in Azerbaijan. According to DOE officials, new implementing agreements with the appropriate ministries or agencies within the governments of each of the countries where the old equipment is located are needed before DOE can install more sophisticated equipment. According to DOE officials, these agreements are important because they exempt DOE from paying foreign taxes and require host governments to provide DOE with data on detections of illicit trafficking in nuclear materials. Until these border sites receive equipment with both gamma and neutron detection capability, they will remain vulnerable to certain forms of nuclear smuggling.

- Regarding problems with equipment maintenance, DOE has not systematically maintained handheld radiation detection equipment provided by State and other agencies. As a result, many pieces of handheld equipment, which are vital for border officials to conduct secondary inspections of vehicles or pedestrians, may not function properly. For example, in Georgia, we observed border guards performing secondary inspections with a handheld radiation detector that had not been calibrated (adjusted to conform with measurement standards) since 1997. According to the detector's manufacturer, yearly recalibration is necessary to ensure that the detector functions properly.

- Finally, many border sites are located in remote areas that often do not have access to reliable supplies of electricity, fiber optic lines, and other infrastructure essential to operate radiation detection equipment and associated communication systems. Additionally, environmental conditions at some sites, such as extreme heat, can affect the performance of equipment. To mitigate these concerns, DOE, DOD, and State have provided generators and other equipment at remote border sites to ensure stable supplies of electricity and, when appropriate, heat shields or other protection to ensure the effectiveness of radiation detection equipment.

State has taken some steps to coordinate U.S. radiation detection equipment assistance overseas, but its ability to carry out its role as lead coordinator is limited by shortcomings in its strategic plan for interagency coordination and by its lack of a comprehensive list of all U.S. radiation detection equipment assistance. In response to a recommendation we made in 2002, State led the development of a governmentwide plan to coordinate U.S. radiation detection equipment assistance overseas. This plan broadly defines a set of interagency goals and outlines the roles and responsibilities of participating agencies. However, the plan lacks key components we recommended, including overall program cost estimates, projected time frames for program completion, and specific performance measures. Without these elements in the plan, State will be limited in its ability to effectively measure U.S. programs' progress toward achieving the interagency goals. Additionally, in its role as lead interagency coordinator, State has not maintained accurate information on the operational status and location of all radiation detection equipment provided by U.S. programs. While DOE has responsibility for maintaining information on previously deployed U.S.-funded portal monitors, State primarily works through its in-country advisors to gather and maintain information on handheld radiation detection equipment provided by State and other U.S.

agencies. However, four of nine in-country advisors we spoke with, who are stationed in countries that have received significant amounts of handheld radiation detection equipment, said that they did not have up-to-date information regarding the operational status and location of this equipment. Furthermore, while DOE, DOD, and State each maintain lists of radiation detection equipment provided by their programs, they do not regularly share such information, and there is no comprehensive list of all equipment provided by U.S. programs. Without such a coordinated master list, program managers at DOE, DOD, and State cannot accurately assess if equipment is operational and being used as intended; determine the equipment needs of countries where they plan to provide assistance; or detect whether an agency has unknowingly supplied duplicative equipment.

To strengthen program management and effectiveness, we recommend that the Secretary of Energy, working with the Administrator of the National Nuclear Security Administration, revise the long-term cost projections for the SLD-Core program to account for the cost of providing specific anticorruption measures and upgrade portal monitors previously provided by other U.S. government agencies and currently maintained by DOE that do not have both gamma and neutron detection capability as soon as possible. Additionally, to strengthen accountability of U.S. radiation detection assistance programs, we recommend that the Secretary of State, working with the Secretaries of Defense and Energy and the Administrator of the National Nuclear Security Administration, ensure maintenance is provided for all handheld radiation detection equipment supplied by U.S. programs; strengthen the *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* by including specific performance measures, overall cost estimates, and projected time frames for completion of U.S. efforts; and compile, maintain, and share a master list of all U.S. radiation detection assistance.

We provided the Departments of Energy, Defense, and State with draft copies of this report for their review and comment. DOE and State generally agreed with our conclusions and recommendations. DOD had no written comments on our report. DOE provided additional information clarifying its prioritization process, anticorruption measures, and maintenance efforts. State disagreed with our emphasis on the interagency working group and in-country advisors as the primary mechanisms for coordination of U.S. radiation detection equipment assistance programs. State believes that informal coordination between State program officers and their interagency counterparts in Washington, D.C., is the primary

coordination mechanism. We have added language that notes the existence of such informal coordination. However, State's own *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* does not mention such informal mechanisms. Rather, State's plan emphasizes the role of the interagency working group and states that such coordination is "vital to the overall success of U.S. nuclear detection assistance efforts." DOE, DOD, and State also provided technical comments, which we incorporated as appropriate.

Background

Since our May 2002 report on nuclear smuggling, the International Atomic Energy Agency (IAEA) has reported 481 additional confirmed cases of the smuggling of nuclear and/or radiological materials.[6] One of these cases involved nuclear material suitable for use in a nuclear weapon.[7] The majority of new cases IAEA reported involved radiological sources, which could be combined with conventional explosives to create a "dirty bomb." According to IAEA, the majority of all reported incidents with radiological sources involved criminal activity, most frequently theft. Radiological sources and devices in which they are used can be attractive for thieves because of their perceived high resale value or the value of their ability to shield or encapsulate illegally shipped materials within legal shipments of radioactive materials. Some of the reported cases indicate a perceived demand for radioactive materials on the black market, according to IAEA. From 2003 to 2004, the number of incidents reported by IAEA substantially increased. IAEA indicated that improved reporting may, in part, account for this increase. As of December 2004, 82 of IAEA's Member States were participating in contributing to the database.[8]

Detecting actual cases of illicit trafficking in nuclear material is complicated because one of the materials of greatest concern—highly enriched uranium—is among the most difficult materials to detect because

[6]IAEA's database includes incidents involving unauthorized acquisition, provision, possession, use, transfer, or disposal of nuclear materials or other radioactive materials, whether intentional or unintentional and with or without crossing international borders, including unsuccessful and thwarted events. These include incidents involving loss and discovery of uncontrolled nuclear and radiological materials.

[7]According to IAEA, in June 2003, an individual was arrested while attempting to smuggle 170 grams of highly enriched uranium across the border between Armenia and Georgia.

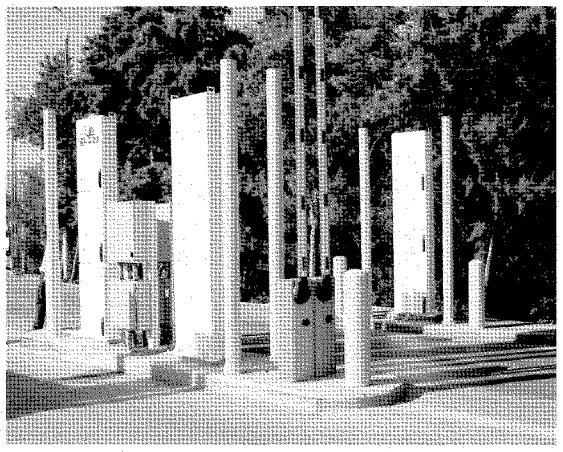
[8]It is important to note that participation in IAEA's nuclear trafficking database is voluntary.

of its relatively low level of radioactivity. Uranium emits only gamma radiation so detection equipment, which generally contains both gamma and neutron detection capabilities, only detects uranium from the gamma detector. However, gamma radiation emissions can be shielded by encasing nuclear material within another high density material, such as lead. Another nuclear material of great concern is plutonium, which emits both gamma and neutron radiation. However, shielding nuclear material generally does not prevent the detection of neutron radiation and, as a result, plutonium can be detected by neutron detectors regardless of the amount of shielding from high density material. According to DOE officials, neutron radiation alarms are only caused by man-made materials, such as plutonium, while gamma radiation alarms are caused by a variety of naturally occurring sources including commercial goods such as bananas, ceramic tiles, and fertilizer, in addition to dangerous nuclear materials, such as uranium and plutonium.

The most common types of radiation detection equipment are radiation portal monitors; handheld equipment, including both survey meters and radioactive isotope identification devices; and radiation pagers. The radiation detection equipment that U.S. programs provide to foreign countries is commercially available, off-the-shelf technology. Radiation portal monitors are stationary pieces of equipment designed to detect radioactive materials being carried by vehicles, pedestrians, or railcars. Radiation portal monitors currently being provided by U.S. agencies have the ability to detect both gamma and neutron radiation, which is important for detecting highly enriched uranium and plutonium, respectively. According to DOE, radiation portal monitors with both gamma and neutron detectors cost between about $28,000 and $55,000, plus the additional costs associated with installing the equipment and communication systems necessary to operate it.[9] Figure 1 shows a picture of radiation portal monitors with both gamma and neutron detectors.

[9]The price of radiation portal monitors varies depending on the manufacturer and type of monitor, e.g., whether the portal monitor is built to screen pedestrians, vehicles, or trains.

Figure 1: Radiation Portal Monitors Containing Both Gamma and Neutron Radiation Detectors at a Border Site in Northern Greece



Source: GAO.

In 2002, we reported that some U.S. agencies, primarily State, provided radiation portal monitors that did not have the ability to detect neutron radiation to foreign governments.[10] Because this equipment is capable of detecting only gamma radiation, it is less effective in detecting certain nuclear material, such as plutonium that has been shielded with high density material. Replacement cost for similar equipment (capable of detecting only gamma radiation), is about $5,000, not including installation costs, according to DOE officials. Figure 2 shows an example of such a radiation portal monitor.

[10]See GAO-02-426.

Figure 2: Older Radiation Portal Monitor Able to Detect Only Gamma Radiation at a Border Site in Georgia

Source: GAO.

Handheld radiation detection equipment, such as survey meters and radioactive isotope identification devices, are used by customs officials and border guards to conduct secondary inspections,[11] the aim of which is to localize the source of an alarm and determine the nature of the material present. Survey meters can be used to detect the level of radiation by providing a count of the radiation level in the area. Radioactive isotope identification devices, commonly known as RIIDs, identify the specific isotope of the radioactive source detected. In addition, U.S. programs often provide radiation pagers, which are small radiation detection devices worn on belts by border security personnel to continuously monitor levels of radiation in the area. Pagers are considered personal safety devices and, therefore, should not be relied upon to implement secondary inspections.[12]

Three U.S. Agencies Have Spent About $178 Million to Provide Radiation Detection Equipment to 36 Countries, but Future Spending Requirements for Some Programs Are Uncertain

Since fiscal year 1994, DOE, DOD, and State have spent about $178 million to provide radiation detection equipment to 36 countries as part of the overall U.S. effort to combat nuclear smuggling. However, because some U.S. agencies provide radiation detection equipment to foreign countries on an as needed basis, future U.S. government spending requirements for such assistance are uncertain.

[11]Primary inspections are conducted with radiation portal monitors to determine whether there is a presence of radiation. After radiation is detected, a secondary inspection is conducted to determine where the source is located and what material is present.

[12]Handheld radiation detection equipment is generally less expensive than fixed radiation portal monitors, in part, because there are no installation costs associated with providing handheld equipment. According to DOE, DOD, State, and DHS officials, survey meters cost about $1,200 to $7,000; RIIDs typically cost about $3,000 to $18,000; and radiation pagers cost about $1,500.

DOE, DOD, and State Had Spent a Combined Total of About $178 Million through the End of Fiscal Year 2005 to Provide Radiation Detection Equipment to 36 Countries

DOE has spent about $131 million to provide radiation detection equipment and training to 12 countries and to maintain certain types of equipment previously installed by other U.S. agencies in 23 countries. DOD has also spent almost $22 million to provide radiation portal monitors, handheld radiation detection devices, and radiation detection training to 8 countries in the former Soviet Union and Eastern Europe. Similarly, State has spent about $25 million to provide various types of radiation detection equipment and related training to 31 countries. (See table 1.)

Table 1: U.S. Spending by Program on Radiation Detection Equipment and Related Training Provided to Foreign Countries through the End of Fiscal Year 2005

Dollars in millions

Agency	Program	Expenditures
DOE	Second Line of Defense "Core" program	$129.5
DOE	Cooperative Radiological Instrument Transfer project	1.2
DOD	Weapons of Mass Destruction Proliferation Prevention Initiative	7.9
DOD	International Counterproliferation Program	14.5
State	Export Control and Related Border Security program	15.4
State	Nonproliferation and Disarmament Fund	9.1
State	Georgia Border Security and Law Enforcement program	0.2
Total		**$177.8**

Sources: GAO analysis of DOD, DOE, and State data.

Note: Figures have been rounded.

DOE Has Spent About $131 Million Providing Radiation Detection Equipment and Related Training

Since fiscal year 1998, DOE has spent about $130 million through its SLD-Core program to provide radiation detection equipment and training at 83 border sites in Russia, Greece, and Lithuania and to maintain certain types of equipment previously installed by State and other U.S. agencies in 23 countries.[13] DOE recently signed implementing agreements with the governments of Azerbaijan, Georgia, Slovenia, and Ukraine and will begin work in those countries in fiscal year 2006. Through its SLD-Core program,

[13]From fiscal year 1997 through fiscal year 2001, State provided DOE with approximately $2.7 million to assist its SLD-Core program with installing radiation detection equipment at eight sites in Russia. These sites included an airport near Moscow, six seaports, and one railroad crossing. We have included the $2.7 million provided by State under total expenditures for DOE.

DOE currently plans to install radiation detection equipment at a total of about 350 sites in 31 countries by 2012 at an estimated total cost of $570 million.

In addition, DOE spent about $1 million to provide radiation detection equipment to nine countries through its Cooperative Radiological Instrument Transfer project (CRITr), which began in 2004. Through CRITr, DOE refurbishes previously decommissioned handheld radiation detection equipment located at various DOE sites and provides this equipment to foreign law enforcement officers. DOE plans to provide handheld equipment to six additional countries through the CRITr project in fiscal year 2006.[14]

DOD Has Spent About $22 Million to Provide Handheld Radiation Detection Devices to Eight Countries and to Install Portal Monitors in Uzbekistan

Through the end of fiscal year 2005, DOD had spent about $22 million through two programs to provide handheld radiation detection devices to eight countries in the former Soviet Union and Eastern Europe and to install fixed radiation portal monitors in Uzbekistan. Specifically, through its Weapons of Mass Destruction Proliferation Prevention Initiative (WMD-PPI), DOD spent about $0.2 million to provide various types of handheld radiation detection equipment to three countries and about $6.4 million to install radiation portal monitors at 11 sites in Uzbekistan.[15] DOD plans to complete installation at 6 more sites in Uzbekistan by the end of fiscal year 2006 and to finish all associated radiation detection work in Uzbekistan by fiscal year 2009 at a total cost of about $54 million. In fiscal year 2006, DOD plans to transfer responsibility for maintenance of the equipment it has provided to Uzbekistan to DOE's SLD-Core program.[16]

Through its International Counterproliferation Program (ICP), DOD has spent about $15 million to provide handheld radiation detection equipment

[14]Additional information on these DOE radiation detection assistance programs can be found in appendix II.

[15]The program spending total for DOD's WMD-PPI program is misleading because, in addition to about $6 million in expenditures, DOD has obligated over $19 million to three contracts for program costs associated with installing radiation detection equipment in Uzbekistan, such as communication systems and training. Because DOD only executes spending on these contracts after all work has been completed, these contracts were not paid until fiscal year 2006 and, therefore, are not included in the program's expenditure total.

[16]According to DOE officials, DOE's SLD-Core program has worked with DOD to coordinate on the types of radiation detection equipment and specific sites in Uzbekistan that will receive assistance.

and training on weapons of mass destruction proliferation prevention to 6 countries in the former Soviet Union and Eastern Europe. In addition, DOD has provided a variety of training on weapons of mass destruction proliferation to 17 additional countries. Through ICP, DOD plans to continue to provide limited amounts of handheld radiation detection equipment to other countries in the future.[17]

State Has Spent About $25 Million to Provide Radiation Detection Equipment and Related Training to 31 Countries

The Department of State, through three programs—the Export Control and Related Border Security program (EXBS), the Nonproliferation and Disarmament Fund (NDF), and the Georgia Border Security and Law Enforcement program (GBSLE)—has spent about $25 million since fiscal year 1994 to provide radiation detection equipment and related training to 31 foreign countries. State's EXBS program has spent approximately $15.4 million to provide radiation portal monitors, various types of handheld radiation detection devices, X-ray vans equipped with radiation detectors, and training on how to use this equipment to 30 countries mainly in the former Soviet Union and Eastern Europe. Similarly, through NDF, State spent about $9.1 million from fiscal year 1994 through 2001 to, among other things, install portal monitors in countries other than Russia, provide handheld radiation detectors, and provide vans equipped with X-ray machines to countries, including Estonia, Latvia, Lithuania, and Poland. Lastly, through its GBSLE program, State spent $0.2 million in 1999 to provide border guards and customs officials in the Republic of Georgia with 137 radiation pagers. State has not provided any additional radiation detection equipment assistance through NDF since 2001 or through its GBSLE program since 1999.[18]

Future U.S. Spending on Radiation Detection Assistance Is Uncertain

Because some U.S. programs provide radiation detection equipment to foreign countries on an as needed basis and DOE has yet to gain agreements with all of the countries where it would like to install equipment, future U.S. government spending requirements for radiation detection assistance remain uncertain. For example, although DOE is the primary U.S. agency responsible for installing radiation portal monitors in foreign countries, State selectively funds projects to provide radiation

[17]Additional information on these DOD radiation detection assistance programs can be found in appendix III.

[18]For additional information on these radiation detection equipment assistance programs at State, see appendix IV.

portal monitors to foreign countries through its EXBS program. State officials told us that State coordinates its work in this area with DOE to avoid duplication, and it conducts these projects on an as needed basis to provide a quick response to emerging nuclear smuggling threats. For example, in December 2005, State installed portal monitors and provided handheld radiation detection equipment to one site in Armenia at a cost of about $0.5 million, in part because it believed that the threat of nuclear smuggling warranted immediate installation of this equipment. State officials we spoke with told us that they coordinated with DOE to ensure State's work in Armenia is consistent with overall U.S. goals and that the specific equipment installed met minimum detection standards. Furthermore, State officials also told us that the newly installed radiation portal monitors at this site in Armenia provide a redundant layer of security with DOE's planned work to install equipment on the opposite side of the border in the Republic of Georgia.

Because State selectively funds portal monitor projects through its EXBS program to provide a quick U.S. government response to emerging security threats of nuclear smuggling, it is uncertain how many other projects State will fund in this area, in what countries these projects will be conducted, or how much they will cost. Additionally, State officials also told us that they have yet to determine whether or not they will fund any future projects to provide radiation detection equipment assistance to foreign countries through the Nonproliferation and Disarmament Fund or the Georgia Border Security and Law Enforcement program. As a result, it is uncertain how many other projects State will fund through either of these two programs or how much they will cost.

DOE currently plans to install equipment at a total of about 350 sites in 31 countries by 2012 at an estimated cost of $570 million based on a strategy that analyzes and prioritizes countries for receiving installations. However, it cannot be certain which countries will be included in the SLD-Core program until it signs the necessary agreements with these countries' governments. For example, DOE planned to complete installations in Georgia, Kazakhstan, Slovenia, and Ukraine in fiscal year 2005. However, installations in Georgia, Slovenia, and Ukraine will not be completed until at least fiscal year 2006 because of delays in signing implementing agreements with these countries. Additionally, DOE is still in the process of trying to reach agreement with Kazakhstan. In fiscal year 2004, DOE reallocated a portion of its funding to directly fund its planned work at certain border sites in Kazakhstan. However, difficulty in reaching agreement with Kazakhstan continues to delay this work. If DOE continues

to experience delays in signing agreements with foreign countries, or cannot reach agreements with all of the countries where it currently plans to install equipment, it may need to alter its planned scope of work and overall cost estimates for the program. Furthermore, once DOE reaches agreement with a certain country, it still needs to conduct individual site assessments to determine at which sites providing radiation detection equipment will be cost-effective, as well as the amount of equipment each site will require. Therefore, DOE is limited in its ability to determine the total cost of the SLD-Core program until it signs implementing agreements with the governments of countries where it plans to work and conducts assessments to determine which specific sites within those countries require radiation detection equipment and in what amounts.

The Threat of Corruption, Technological Limitations, Maintenance Problems, and Site Infrastructure Issues Challenge U.S. Programs to Combat Nuclear Smuggling

U.S. programs that provide radiation detection equipment to foreign governments face a number of challenges that affect the installation and effective operation of radiation detection equipment, including: the threat of corruption of border security officials in some foreign countries, technical limitations of radiation detection equipment previously deployed by State and other agencies, inadequate maintenance of some handheld equipment, and the lack of infrastructure necessary to operate radiation detection equipment and harsh environmental conditions at some border sites. DOE, DOD, and State have taken some steps to address these challenges, such as providing multitiered communications systems to mitigate corruption so that alarm data can be simultaneously viewed at several levels of authority and supplying protective casings for radiation portal monitors to prevent damage from vandals or extreme heat.

Possible Corruption of Border Guards Poses a Threat to the Effective Operation of U.S.-Funded Radiation Detection Equipment

According to U.S. and foreign government officials, corruption is a pervasive problem within the ranks of border security organizations. Specifically, because foreign border guards are often poorly paid and geographically isolated, there are concerns that foreign officials could be bribed and turn off the radiation detection equipment and allow nuclear smuggling to occur. For example, an official might turn off the equipment to allow a nuclear smuggler to pass through a border crossing. According to a Russian press report, in October 2004, a Russian customs agent at a site in western Russia was fired because he was aiding a smuggling ring. Additionally, in July 2005, after the newly elected President of Ukraine took

office, he reorganized many agencies within the government, including the Customs Service, because of concerns about corruption.

DOE, DOD, and State officials told us they are concerned that corrupt foreign border security personnel could compromise the effectiveness of U.S.-funded radiation detection equipment by either turning off equipment or ignoring alarms. As a result, U.S. programs that provide fixed radiation portal monitors are taking some steps to evaluate the degree to which corruption is present in the countries and regions where they are working or plan to work. For example, DOE's SLD-Core program commissioned three studies to better understand corruption and the challenges that it could bring to the program. Additionally, DOE includes countrywide corruption assessments as part of its efforts to help program officials prioritize countries to include in the SLD-Core program. In addition, DOD and State also include anticorruption courses as part of the radiation detection training they provide to foreign border security personnel.

Some U.S. programs also have taken or plan to take other specific steps to mitigate the threat of corruption, such as (1) providing multitiered communications systems so that alarm data can be simultaneously viewed at several levels of authority, (2) implementing programs to combat some of the underlying issues that can lead to corruption through periodic screening of border security personnel, and (3) installing radiation portal monitors on both sides of a particular border if there are concerns about corruption of personnel in these countries. For example, DOE and DOD are deploying communication systems that link the activities at individual border sites with regional and national command centers. By doing so, alarm data can be simultaneously evaluated by officials both at the site and up the chain of command, thus establishing redundant layers of accountability for responding to alarms. As a result, if a local official turns off the radiation detection equipment at a site, higher level officials can quickly be made aware of the incident and investigate the reasons for the alarm. Additionally, DOD plans to implement an Employee Dependability Program in Uzbekistan that includes background checks, personal interviews of applicants, monitoring of performance and behavior, and annual refresher training to combat some of the underlying issues that can lead to corruption among border security personnel. DOE officials told us that they are considering implementing such a screening program in some countries where the SLD-Core program works. Lastly, U.S. programs are installing radiation portal monitors on both sides of some borders to create redundant coverage to increase the likelihood of detection and interdiction. In fiscal year 2006, DOE plans to install radiation portal

monitors at a number of sites in Georgia. At one site in Armenia, across the border from a planned DOE installation, State installed radiation portal monitors in December 2005, in part, because of concerns about corruption on both sides of the border at this location. DOE is also considering employing this type of redundant coverage at other locations throughout Eastern Europe and the former Soviet Union.

While DOE has taken steps to determine the level of corruption in some countries and regions where it works and includes countrywide corruption assessments as part of its prioritization model, DOE is still in the process of determining in what countries it will provide specific anticorruption measures and how much it will cost to do so based on its analysis of the corruption threat. For example, DOE estimates that it will spend about $1 million to provide radiation detection equipment and related communications systems at a typical foreign border crossing. DOE officials noted that the standard communication systems the SLD-Core program provides with radiation portal monitors have some anticorruption value because radiation alarms require more than one official to review and close out before the system can be reset. However, DOE has not included the costs associated with other specific anticorruption measures in the long-term cost estimates for its SLD-Core program.

Some Border Crossings Remain More Vulnerable to Nuclear Smuggling Because DOE Has Not Upgraded Less Sophisticated Equipment Installed by Other U.S. Agencies

In 2002, DOE assumed responsibility for maintaining some radiation detection equipment previously installed by State and other U.S. agencies in 23 countries in the former Soviet Union and Eastern Europe. However, DOE has not upgraded any of this less sophisticated equipment, with the exception of one site in Azerbaijan.[19] Through an interagency agreement, DOE assumed responsibility for ensuring the long-term sustainability and continued operation of radiation portal monitors and X-ray vans equipped with radiation detectors that State and other U.S. agencies provided to these countries. Through this agreement, DOE provides spare parts, preventative maintenance, and repairs for the equipment through regularly scheduled maintenance visits. Through the end of fiscal year 2005, DOE had conducted maintenance and sustainability activities for equipment in 21 of the 23 countries where equipment had been provided. DOE officials told us that, although Belarus received a significant amount of radiation detection equipment from DOD, DOE is currently prohibited from

[19]DOE completed upgrading one site in Azerbaijan in December 2005 at a cost of about $86,000.

maintaining this equipment by restrictions placed on U.S. assistance to Belarus.[20] As a result, the maintenance status of the 38 portal monitors and almost 200 pieces of handheld radiation detection equipment DOD provided to Belarus is unknown. Additionally, at the request of the Turkish government, DOE no longer maintains 41 portal monitors and over 150 pieces of handheld radiation detection equipment State previously provided to Turkey.

As we originally reported in 2002, at some sites in foreign countries, State and other U.S. agencies installed portal monitors that contained only gamma radiation detectors, which are less effective in detecting certain nuclear material, such as plutonium, than detectors with both gamma and neutron detection capability. Although State's current policy is to install radiation detection equipment with both gamma and neutron detection capability, according to DOE officials, because of their configuration and sensitivity, these older portal monitors are less likely to detect small quantities of highly enriched uranium or nuclear material that is shielded, for example, by a lead container or certain parts of a vehicle. When it assumed responsibility for maintaining this equipment, DOE conducted an initial assessment of these portal monitors to determine whether they were functional and what maintenance was required. During the course of this analysis, DOE found that much of the equipment was damaged and required total replacement or major repairs. In such cases, DOE installed similar equipment with gamma radiation detectors but chose not to upgrade the equipment with newer portal monitors that would be capable of detecting both gamma and neutron radiation. DOE's policy was to replace this equipment in-kind and wait to upgrade the equipment as part of a countrywide deployment through the SLD-Core program. However, according to SLD-Core program officials, DOE did not have funds earmarked for upgrading the equipment in the absence of a countrywide deployment through the SLD-Core program.

Additionally, SLD-Core program officials stated that DOE would need to sign new agreements with the appropriate ministries or agencies within the governments of the countries where State and other agencies had previously installed equipment before DOE could invest "substantial resources" to upgrade the equipment. DOE officials noted that replacing the less sophisticated portal monitors with similar equipment usually costs

[20]State's Selective Engagement Policy prohibits a variety of U.S. assistance to Belarus and was applied to that country beginning in 1997.

less than $5,000, plus installation costs, while deploying a comprehensive system comprised of portal monitors that can detect both gamma and neutron radiation, associated communication systems, and related training can cost up to $1 million per site. The agreements are important because they exempt DOE from payment of host government taxes, customs duties, or other charges per congressional guidance. In addition, these agreements require the host government to provide DOE with data on detections of illicit trafficking in nuclear materials gathered as a result of assistance DOE provided through the SLD-Core program. Though the SLD-Core program has signed agreements with some countries where the less sophisticated equipment was installed, such as Ukraine, DOE has yet to upgrade any of the equipment in these countries, with the exception of one site in Azerbaijan, primarily because the details of the countrywide installations are still being determined. According to DOE officials, as countries with older equipment sign agreements with DOE to implement the full SLD-Core program, sites in these countries with less sophisticated equipment will be upgraded.

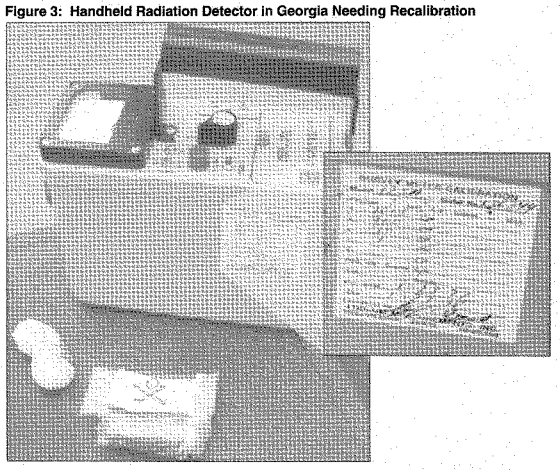
In November 2005, DOE completed an assessment of the maintenance activities it performs on equipment provided by other U.S. agencies. DOE found that equipment failures at many of these sites go unattended, often for months. DOE determined that its maintenance of X-ray vans previously provided by State was not critical to the mission of the SLD-Core program. As a result, DOE is planning to phase out its maintenance of X-ray vans after fiscal year 2007. According to DOE officials, the budget of the SLD-Core program cannot sustain what DOE considers "non-mission critical work." In fiscal year 2005, DOE bore the full financial responsibility for all maintenance activities because State provided no funding to DOE for this work. In addition to the X-ray vans, DOE evaluated the sites where portal monitors were previously installed by State and other agencies and identified those monitors that should no longer be supported by the SLD-Core program. DOE assessed each location where less sophisticated portal monitors are maintained and prioritized which sites should receive upgraded equipment. DOE plans to work with State to upgrade selected sites and decommission some sites that have equipment that is not being used or is beyond repair.

Concerns Exist About Maintenance of Some Handheld Radiation Detection Equipment

DOE and State signed an interagency agreement in 2002 giving responsibility for maintaining most radiation detection equipment previously installed by State and other U.S. agencies to DOE. However, this agreement did not make DOE responsible for maintaining handheld radiation detection equipment previously deployed by these agencies. State has also not assumed responsibility for maintaining about 1,000 handheld radiation detectors provided by its programs that are vital to border officials for conducting secondary inspections of vehicles and pedestrians, and, as a result, much of this equipment is in disrepair.[21] For example, at one site in Georgia, we observed border guards performing secondary inspections with a handheld radiation detector, previously provided by State, which had not been calibrated since 1997 (see fig. 3). According to the detector's manufacturer, yearly recalibration is necessary to ensure that the detector functions properly. Furthermore, DOE officials we spoke with told us that—similar to radiation portal monitors—handheld radiation detection devices require periodic maintenance checks and recalibration to ensure that they remain operable and continue to meet minimum detection standards.

[21]In addition to the handheld radiation detection equipment cited above, about 900 radiation pagers were also previously provided by State and other U.S. agencies. However, according to DOE and State officials, radiation pagers generally require little maintenance and have a relatively low replacement cost compared with radioactive isotope identification devices or other handheld radiation detection equipment used for conducting secondary inspections.

Figure 3: Handheld Radiation Detector in Georgia Needing Recalibration



Source: GAO.

Batteries used in some handheld radiation detection equipment typically need to be replaced every 2 years and some types of handhelds are fragile and can be easily broken, requiring that replacement devices or spare parts be readily available. At the request of State, DOE is currently evaluating the costs associated with maintaining this handheld equipment. Specifically, DOE has asked its contractor currently responsible for maintaining the portal monitors and X-ray vans in these countries to develop a proposal for assuming responsibility for maintenance of the handheld equipment as well. According to DOE officials, maintenance of handheld equipment could be conducted during regularly scheduled visits for maintenance of

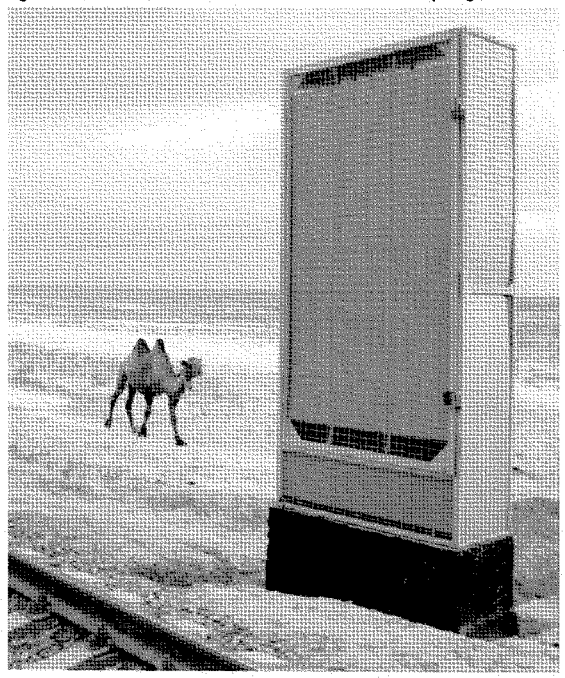
portal monitors and X-ray vans.[22] As a result, DOE officials believe that no additional travel funds would be required for this activity. However, DOE officials also told us that if they were to assume full responsibility for maintaining the handheld equipment at sites where they are maintaining radiation portal monitors installed by State and other agencies they would need additional funding for labor and to provide replacement equipment and spare parts.

Limited Infrastructure and Harsh Environmental Conditions at Some Border Sites Pose Equipment Problems

Limited infrastructure and harsh environmental conditions at some foreign border sites create challenges to the installation and operation of radiation detection equipment. For example, many border sites are located in remote areas, which often do not have access to reliable supplies of electricity, fiber optic lines, and other infrastructure needed to operate radiation portal monitors and associated communication systems. Prior to providing radiation portal monitors, U.S. programs typically perform site assessments to determine the details surrounding how radiation detection equipment will be installed at a given site. The assessment includes the operational needs of the equipment depending on the infrastructure available at the site. To address the needs identified, DOE, DOD, and State provide generators at some sites to supply electricity to the radiation detection equipment because the electric power supply shuts down periodically or may be very low at these remote sites. Additionally, the communication systems that are provided to report activities from the radiation detectors require fiber optic cabling for their operation. If no cabling exists, underground cabling or radio wave operated communication systems must be installed to perform this function. Finally, at some border sites, the radiation portal monitors are located significant distances from the control and communication system center. U.S. program officials we spoke with expressed concern that theft could occur because of the remote location of this equipment. To prevent such interference with the equipment, antitampering measures such as protective cages are used to protect the integrity of the portal monitors (see fig. 4).

[22]DOE officials noted that, during regular site visits to conduct maintenance on radiation portal monitors, DOE maintenance teams often are asked by the host government to maintain handheld radiation detection equipment provided by other U.S. programs. DOE officials also stated that although this work is outside the scope of DOE's responsibility, when time and funding permit, DOE maintenance teams have replaced some dysfunctional equipment on a case-by-case basis.

Figure 4: Rail Portal Monitor in Western Uzbekistan with Antitampering Protection



Source: DOD.

Additionally, environmental conditions at some sites, such as extreme heat, can compromise the effectiveness of radiation detection equipment. Extreme heat can accelerate the degradation of components within

radiation detection equipment and, as a result, can affect the performance and long-term sustainability of the equipment. DOD placed a protective casing around the radiation portal monitors it installed in Uzbekistan as a heat shield to ensure the effective long-term operation of the equipment (see fig. 5).

Figure 5: Radiation Portal Monitor in Uzbekistan with Heat Shield Enclosure

Source: GAO.

State's Efforts to Coordinate U.S. Assistance Are Limited by Deficiencies in the Interagency Strategic Plan and the Lack of a Comprehensive List of Equipment Provided by U.S. Programs

State coordinates U.S. radiation detection equipment assistance overseas through an interagency working group and in-country advisors. However, its ability to carry out its role as lead interagency coordinator is limited by deficiencies in the strategic plan for interagency coordination and by its lack of a comprehensive list of all U.S. radiation detection assistance. Specifically, the interagency strategic plan lacks key components, such as overall program cost estimates, projected time frames for program completion, and specific performance measures. Additionally, State has not maintained accurate information on the operational status and location of all radiation detection equipment provided by U.S. programs.

State Coordinates U.S. Radiation Detection Equipment Assistance through an Interagency Working Group and In-Country Advisors

As the lead coordinator of U.S. radiation detection equipment assistance overseas, State has taken some steps to coordinate the efforts of U.S. programs that provide this type of assistance to foreign countries. State's coordination takes place primarily through two methods: an interagency working group and State's in-country advisors. The main coordination mechanism for U.S. radiation detection assistance programs is the interagency working group, chaired by State, which consists of program representatives from DOE, DOD, State, and DHS. According to State, this working group holds meetings about once every 2 months to coordinate the activities of U.S. programs that provide radiation detection equipment and export control assistance overseas. These interagency meetings attempt to identify and prevent overlap among the various U.S. programs through discussion of such issues as funding, upcoming program activities, and recent trips to countries receiving U.S. assistance. Meetings are attended by program managers responsible for overseeing and implementing radiation detection equipment assistance programs in foreign countries. While DOD and DOE officials we spoke with told us that these interagency meetings are somewhat beneficial, they stated that meetings primarily facilitate coordination at a high level and typically lack the specific detail necessary to identify and prevent program overlap within countries and regions where multiple U.S. programs provide radiation detection equipment assistance. Through this working group, State also maintains an interagency schedule that provides information on planned activities, training, and site visits of U.S. programs.

State also coordinates U.S. programs through in-country advisors, stationed in more than 20 foreign countries. While State funds these

advisors, State officials told us that they work on behalf of all U.S. programs that provide nuclear detection assistance in their respective countries. According to State officials, these advisors serve as the on-the-ground coordinators of U.S. export control and border security assistance and are the primary sources of information concerning past and present provision of U.S. radiation detection equipment assistance in their respective countries. State officials also noted that frequent informal coordination takes place between program managers at State and their counterparts in Washington, D.C., at other federal agencies.

In addition to State's coordination efforts, DHS recently created the Domestic Nuclear Detection Office (DNDO) with responsibilities including coordinating nuclear detection research and developing a global nuclear detection architecture.[23] According to DHS, though DNDO is principally focused on domestic detection, its coordinating work will enhance U.S. efforts overseas through the design of a global nuclear detection architecture implemented under current agency responsibilities. Equally, while detection technologies developed by DNDO will be directed primarily by operational requirements for domestic applications, many technologies developed could have application in overseas radiation detection equipment assistance programs. However, DOE, DOD, and State officials we spoke with were unclear on what specific future role DNDO would play in coordinating activities of U.S. programs that provide radiation detection equipment assistance to foreign countries. These agencies are working with DNDO to clarify the future role that the office will play.

The Interagency Strategic Plan to Coordinate U.S. Radiation Detection Equipment Assistance Overseas Lacks Key Components

In 2002, we reported that U.S. efforts to help other countries combat nuclear smuggling needed strengthened coordination and planning to link U.S. programs through common goals and objectives, strategies and time frames for providing assistance, and performance measures for evaluating

[23]According to DHS, other responsibilities of DNDO include the (1) acquisition and support-to-deployment of the domestic detection system, (2) enhancement of effective sharing and use of nuclear detection-related information and intelligence, and (3) establishment of procedures and training for the end users of equipment developed and deployed through the new office.

the effectiveness of U.S. assistance.[24] State, as the lead coordinator of U.S. nuclear detection assistance overseas, led the development of a governmentwide interagency strategic plan to guide the efforts of U.S. programs that provide this assistance.[25] The plan broadly defines a set of interagency goals and objectives, establishes minimum technological standards for radiation detection equipment that U.S. programs provide, and outlines the roles and responsibilities of each agency. However, the plan does not include several elements necessary to effectively link U.S. programs together, prevent duplication, and guide their efforts toward completion.

While the plan provides U.S. agencies with a broad framework for coordinating this type of assistance by defining a set of interagency goals and outlining the roles and responsibilities of each agency, it does not include specific performance measures, overall program cost estimates, or projected time frames for program completion. Without incorporating these key elements into its plan, State will be limited in its ability, as lead coordinator, to effectively link U.S. programs and guide their efforts toward achieving interagency goals. For example, a primary goal in its plan is that recipient countries possess a comprehensive capability to detect and interdict illicitly trafficked nuclear and radiological material. However, without incorporating specific performance measures into its plan, State has no transparent way to effectively measure the performance of U.S. programs in this regard or to determine the degree to which they are reaching this or other interagency goals discussed in its plan. Finally, without incorporating overall program cost estimates and time frames for program completion into its plan, State cannot effectively determine the amount of U.S. government resources that will be required to achieve interagency goals and objectives or under what time frames these resources will be required. If State does not take steps to include these key elements in its plan, it will continue to be limited in its ability to effectively track the progress of U.S. programs, measure their performance toward achieving interagency goals and objectives, and determine the amount of

[24]For additional details on the findings and recommendations discussed in our prior report, see GAO-02-426.

[25]The *Strategic Plan For Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* is intended to complement the existing program management plans of all participating agencies, which include DOE, DOD, State, DHS, and the Department of Commerce. DHS and Commerce are implementers of parts of State's EXBS program and thus were included as signatories to the plan.

funding required to achieve these goals and under what time frames these resources will be needed.

State Has Not Maintained Accurate Information on All Previously Provided Handheld Equipment, Which Inhibits Its Ability to Effectively Coordinate U.S. Assistance

State, in its role as lead interagency coordinator, has not maintained accurate information on the operational status and location of all the handheld radiation detection equipment previously provided by U.S. programs. While DOE has taken responsibility for maintaining information on previously deployed U.S.-funded radiation portal monitors, State primarily works through its in-country advisors and its interagency working group to gather and maintain information on handheld radiation detection equipment provided by U.S. programs. State, through its EXBS program, assumed direct management of the in-country advisors from DHS in February 2005. As part of their duties, State's in-country advisors are required to maintain a record of the transfer of all U.S.-provided export/border control equipment, including radiation detection equipment, within their respective countries and to follow up to ensure it is at the locations specified by the recipient government and is properly maintained. However, four of the nine advisors we spoke with, who are stationed in countries that have received a combined total of about 1,000 pieces of handheld radiation detection equipment from U.S. programs, acknowledged that they did not have up-to-date information regarding the present operational status or location of this equipment. Additionally, five of nine advisors we spoke with were unaware that, as part of their duties, they are required to maintain a record of all U.S.-provided equipment within their country. However, some advisors we spoke with stated that they attempt to determine this information but are sometimes limited in their ability to do so because other U.S. programs have not always coordinated with them before providing equipment in their country. As a result, it is necessary for some advisors to follow up with the host government to determine the status and location of U.S.-provided radiation detection equipment. According to some advisors, however, host governments may not always provide accurate information on what equipment has been provided in the past, where it is currently located, and its current operational status.

According to State officials, there is no comprehensive interagency list of radiation detection equipment that has been previously provided to foreign governments by U.S. programs. In 2002, we recommended that State, as the lead interagency coordinator, work with DOE and DOD to develop such a list. Officials we spoke with at DOE and DOD stated that having access to accurate information on past provisions of all radiation detection

equipment provided by U.S. programs is essential to interagency coordination, preventing overlap among programs, as well as appropriately assessing a specific country's equipment needs. During the course of our review, program officials at DOE, DOD, and State provided us with lists of radiation detection equipment their programs had provided to other countries. According to information we received from program managers at DOE, DOD, and State, more than 7,000 pieces of handheld radiation detection equipment, including radiation pagers and radioactive isotope identification devices, had been provided to 36 foreign countries through the end of fiscal year 2005. Because much of this equipment was provided to the same countries by multiple agencies and programs, it is difficult to determine the degree to which duplication of effort has occurred. For example, since fiscal year 1994, a total of 17 different countries have received handheld radiation detection equipment from more than one U.S. agency. However, although DOE, DOD, and State programs each maintain their own lists of radiation detection equipment provided to foreign countries, officials at these agencies told us that they do not regularly share such information with each other. Without the development of a comprehensive interagency list of U.S.-funded radiation detection equipment, program managers at DOE, DOD, and State cannot accurately assess the equipment needs of countries where they plan to provide assistance, may unknowingly provide duplicative sets of equipment, and cannot determine if the equipment is being used for its intended purpose or is in need of maintenance and repair.

Conclusions

Since the mid-1990s, DOE, DOD, and State have spent about $178 million to provide a variety of radiation detection equipment to countries around the world, and it is important that this equipment be properly maintained so that it can be effectively used to combat nuclear smuggling overseas. Since taking over responsibility for maintaining portal monitors deployed by other agencies in 2002, DOE has worked to ensure that this equipment is functioning and being used as intended. However, because DOE's interagency maintenance agreement with State did not include maintaining handheld radiation detection equipment previously provided by State and other agencies, much of this equipment may not be properly functioning. Handheld radiation detection equipment is vital for border officials to conduct secondary inspections of vehicles or pedestrians. Without taking steps to ensure that all previously provided radiation detection equipment, specifically handheld equipment, is adequately maintained and remains operational, State cannot ensure the continued effectiveness or long-term sustainability of this equipment.

Because corrupt officials could undermine the effectiveness of U.S. radiation detection assistance programs overseas by turning off radiation detection equipment or not properly responding to alarms, it is important for U.S. programs to employ anticorruption efforts, such as multitiered communication systems for radiation alarms, training, employee dependability programs, and redundant installations of equipment when providing such assistance. While we are encouraged that DOE, DOD, and State employ some corruption mitigation measures in their programs, DOE is still in the process of determining in which countries it will provide these specific anticorruption measures and how much such assistance would cost to implement.

In addition, though DOE has maintained less sophisticated radiation portal monitors previously deployed by other agencies since 2002, it has not upgraded the equipment at any of these sites. As a result, border sites with less sophisticated radiation portal monitors are more vulnerable to nuclear smuggling than sites with equipment that can detect both gamma and neutron radiation. We originally reported on this problem in our May 2002 report. In its official comments on that report, DOE stated that these less sophisticated monitors "are not as reliable [as monitors with both gamma and neutron radiation detection capabilities], and have limited or no ability to detect shielded plutonium." Although it is encouraging that DOE has recently undertaken an assessment of the equipment it maintains that was installed by other U.S. agencies, DOE has not yet improved the neutron detection capabilities of any of these less sophisticated monitors, with the exception of one site in Azerbaijan. As a result, these sites remain just as vulnerable to certain types of nuclear smuggling as they were when we first reported this deficiency in May 2002.

Finally, we believe that, unless key components such as overall program cost estimates, projected time frames for completion, and specific performance measures are incorporated into the interagency strategic plan, State will be limited in its ability to determine the amount of resources and time needed to achieve the broader interagency goals discussed in its plan or to effectively measure U.S. programs' progress toward achieving these goals. Furthermore, without accurate information on the current status and location of radiation detection equipment previously provided by U.S. programs, State cannot effectively fulfill its role as interagency coordinator of U.S. assistance. Because there are at least seven U.S. programs at three federal agencies that provide radiation detection equipment to foreign countries, program managers at DOE, DOD, and State need access to a "master list" that shows the status and location

of all U.S. radiation detection equipment assistance to more accurately determine the needs of specific countries and to avoid duplication of effort among U.S. programs. Without such a list, the potential exists for programs to provide duplicative sets of radiation detection equipment to the same country.

Recommendations for Executive Action

To strengthen program management and effectiveness, we recommend that the Secretary of Energy, working with the Administrator of the National Nuclear Security Administration, take the following two actions:

- Integrate projected spending on specific anticorruption measures into the long-term cost estimates for the SLD-Core program.
- Upgrade less sophisticated portal monitors previously installed by other U.S. agencies where DOE has determined this to be appropriate as soon as possible and include funding to accomplish this in DOE's planning and budgeting process.

To strengthen accountability of U.S. radiation detection equipment assistance programs, we recommend that the Secretary of State, working with the Secretaries of Defense and Energy and the Administrator of the National Nuclear Security Administration, take the following three actions:

- Ensure continued maintenance of all radiation detection equipment provided to foreign governments, including all handheld equipment previously provided by State and other agencies.
- Strengthen the *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* by including in the plan (1) specific performance measures to more effectively track and measure the progress U.S. programs are making toward achievement of interagency goals and objectives and (2) overall cost estimates and projected time frames for completion of U.S. radiation detection equipment assistance efforts to determine the amount of U.S. government resources required to achieve interagency goals and objectives and under what time frames these resources will be required.
- To the extent possible, account for all U.S.-funded radiation detection equipment provided to foreign governments, especially handheld equipment, by creating, maintaining, and sharing among all agencies a comprehensive list of such assistance.

Agency Comments and Our Evaluation

DOE and State agreed in general with our conclusions and recommendations. DOD had no written comments on our report. DOE, DOD, and State provided technical comments, which we incorporated as appropriate.

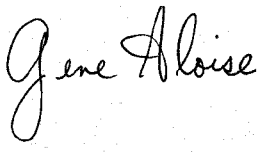
In its comments, DOE wrote that it does not believe that our report adequately reflects the department's efforts to maintain handheld radiation detection equipment provided by State and other agencies because DOE has a process in place to identify and replace handheld equipment used at sites where DOE maintains radiation portal monitors installed by State and other agencies. However, we believe that the extent of DOE's program is fairly presented because this effort does not cover all handheld equipment previously provided by State and other agencies—only equipment at the selected sites visited by DOE's maintenance teams is maintained. Further, the current operational status of the vast majority of handheld radiation detection equipment previously deployed by State and other agencies cannot be determined, in large part, because State has not maintained a comprehensive list of such equipment.

In its comments, State disagreed with our lack of emphasis on the "informal coordination role played by the department's front-line country program officers." State considers informal consultations between these officials and their interagency counterparts to be the "primary means of coordination of its efforts concerning radiation detection equipment provisions." State believes that such informal coordination is "much more important than coordination through the interagency working group or with State's in-country advisors." We have added language to our report noting the role of informal coordination in these programs. However, State's emphasis on them as its primary means of coordinating radiation detection assistance programs conflicts with its own planning documents. In its *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas*, State claims that "a standing sub-working group, the International Nuclear Detection Interagency Working Group, will routinely coordinate nuclear detection, interdiction, and investigation assistance provided by U.S. government agencies." State's plan emphasizes the role of the interagency working group and states that such coordination is "vital to the overall success of U.S. nuclear detection assistance efforts." State's plan does not, however, emphasize or even mention informal coordination mechanisms as a method for State's coordination of U.S. radiation detection assistance programs.

State also believes that its in-country advisors are unfairly criticized for not maintaining comprehensive lists of radiation detection equipment in countries where they are responsible. State cited competing claims on the advisors' time, their many responsibilities within the EXBS program, and the limited resources at their disposal. However, State's own guidance to its in-country advisors states that the advisors' "general duties include…maintaining a record of the transfer of *all* U.S. government-provided nonproliferation export/border control equipment, and following-up to ensure that it is operational, being used for intended purposes at the locations previously specified by the recipient government, and in accordance with U.S. laws and policies."

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. We will then send copies of this report to the Secretary of Energy; the Secretary of Defense; the Secretary of State; the Secretary of Homeland Security; the Administrator, National Nuclear Security Administration; the Director, Office of Management and Budget; and interested congressional committees. We also will make copies available to others upon request. In addition, the report will be made available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-3841 or aloisee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs can be found on the last page of this report. Key contributors to this report include R. Stockton Butler, Julie Chamberlain, Nancy Crothers, Chris Ferencik, Gregory Marchand, and Jim Shafer.



Gene Aloise
Director, Natural Resources and Environment

List of Requesters

The Honorable Susan M. Collins
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Norm Coleman
Chairman
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Carl Levin
Ranking Minority Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Appendix I

Scope and Methodology

We performed our review of U.S. programs that provide radiation detection equipment assistance to foreign countries at the Departments of Energy (DOE), Defense (DOD), Homeland Security (DHS), and State (State) in Washington, D.C.; Los Alamos National Laboratory in Los Alamos, New Mexico; and Sandia National Laboratories in Albuquerque, New Mexico. Additionally, we also visited a "nonprobability" sample of six countries (Georgia, Greece, Macedonia, Russia, Ukraine, and Uzbekistan) where U.S. agencies have provided radiation detection equipment.[1] We visited these six countries to observe U.S.-funded radiation detection equipment in operation and to discuss the implementation of U.S. programs with foreign officials. We determined which specific countries to visit based on several criteria, such as historic U.S. government spending to provide radiation detection equipment within that country; countries receiving radiation detection equipment from multiple U.S. agencies and programs; countries receiving significant amounts of handheld equipment; countries with an in-country advisor stationed at a U.S. Embassy; countries where DOE maintains radiation detection equipment previously installed by State and other U.S. agencies; the current political environment within the country; and our ability to travel from country to county within a reasonable amount of time.

To address the progress U.S. programs have made in providing radiation detection equipment assistance to foreign countries, we reviewed documents and had discussions with officials from DOE's Second Line of Defense "Core" (SLD-Core) program, Cooperative Radiological Instrument Transfer project, and International Nuclear Export Control program; DOE's Office of General Counsel; and DOE's private sector contractors—SI International, Tetra Tech/Foster Wheeler, Bechtel-Nevada, TSA Systems, and Miratek. We also reviewed documents and interviewed relevant officials from DHS's Customs and Border Protection; State's Export Control and Related Border Security (EXBS) program, Nonproliferation and Disarmament Fund, and Georgia Border Security and Law Enforcement program; DOD's Weapons of Mass Destruction Proliferation Prevention Initiative (WMD-PPI), International Counterproliferation Program (ICP), and Defense Threat Reduction Agency; DOD's private sector contractor—Washington Group International; Los Alamos National

[1]Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

Laboratory; Sandia National Laboratories; and Oak Ridge National Laboratory.

In addition, in October 2004, we visited Greece and Macedonia to interview Greek and Macedonian officials and to see U.S. radiation detection assistance provided in each country. In August 2005, we visited Georgia, Russia, Ukraine, and Uzbekistan to see where U.S. agencies have provided radiation detection equipment, to observe U.S.-funded radiation detection equipment in operation, and to discuss the implementation of U.S. programs with foreign officials. We also visited Belgium to meet with officials from the European Union to discuss radiation detection equipment assistance provided to foreign countries by that organization. During our visit to Greece, we spoke with Greek officials from the Greek Atomic Energy Commission; the Greek Ministry of Economy and Finance; and Customs Directorate General (Greek Customs Service). While in Greece, we toured two border crossings where DOE had installed radiation detection equipment through the SLD-Core program, SLD-Core installations at Athens International Airport, and a small research reactor in Athens that received physical security upgrades from DOE prior to the 2004 Olympic Games. While in Macedonia, we interviewed Macedonian officials and toured one border site where radiation detection equipment had previously been provided by the International Atomic Energy Agency and the Department of State.

While in Russia, we spoke with officials from the Federal Customs Service of Russia, ASPECT (a Russian company that develops radiation detection equipment), and DOE officials responsible for implementing the SLD-Core program in Russia. During our visit to Russia, we toured DOE installations at three airports and one seaport, the Federal Customs Service Central Command Center where Russian Customs officials gather and respond to portal monitor alarm data, and the Federal Customs Service Training Academy in Saint Petersburg. While in Uzbekistan, we spoke with officials from DOD's WMD-PPI program, Washington Group International, State and DOD officials at the U.S. Embassy in Tashkent, Uzbekistan's Institute of Nuclear Physics, and the Uzbek State Customs Committee. While in Uzbekistan, we toured the Tashkent Airport and a land border crossing where DOD had provided radiation detection equipment assistance through the WMD-PPI program. We also toured a small research reactor in Uzbekistan that previously received physical security upgrades from DOE, such as barbed-wire fences and video surveillance cameras. During our visit to Georgia, we spoke with officials from State's Georgia Border Security and Law Enforcement program, Department of Georgian State

Border Defense, Georgia Border Security Coordinating Group, and Georgia's Andronikashvili Institute of Nuclear Physics. We toured a land border crossing where State had previously provided radiation detection equipment and visited the Georgian Border Guard Training Academy. While in Ukraine, we spoke with DOE, DOD, and State officials at the U.S. Embassy in Kiev, Ukraine's Border Security Coordinating Group, Ukraine's Border Guard Service, and toured a land border crossing where State had previously provided radiation detection equipment that DOE currently maintains.

We discussed coordination issues with U.S. in-country advisors stationed in countries receiving U.S. assistance, including Armenia, Azerbaijan, Georgia, Kazakhstan, Malta, Moldova, Poland, Romania, and Ukraine. We developed a structured interview guide with a standard set of questions, which we asked all of our interviewees. We designed our interview guide with the assistance of a GAO methodologist. The practical difficulties of asking questions may introduce other types of errors. For example, differences in how a particular question is interpreted or the sources of information available to respondents can introduce unwanted variability into the responses, so we included steps to minimize such errors. We pretested the content and format of the interview guide with two individuals and made minor changes as appropriate.

We chose which specific in-country advisors to interview based on several criteria that include advisors who are stationed in the countries we would be visiting, advisors who are stationed in countries receiving significant amounts of radiation detection equipment from multiple U.S. agencies and programs, and advisors who are stationed in countries where DOE maintains radiation detection equipment previously installed by State and other U.S. agencies. Once we determined which specific advisors to interview, we created a list, which we then randomly ordered to provide an unbiased approach to conducting our interviews. Our goal was to talk with all the advisors on the list, but we knew that circumstances might prevent that so we used a randomized list to provide the order of contacting the advisors. We initiated contact with each advisor from this list, but if we could not establish contact with that advisor, we attempted to establish contact with the next advisor on our list. In some instances, we slightly modified our list due to unforeseen developments. For example, during our visit to the Republic of Georgia, we became aware of a Department of State project to install radiation detection equipment in Armenia opposite the Georgian border. Since this met our criteria for including a country in our pool of interviewees, we agreed it was appropriate, for the purposes of this

review, to add Armenia. We then contacted the in-country advisor stationed in Armenia to learn more about this project. In addition, we removed the responses from the advisor in Russia from our total list of advisors because he failed to respond to more than half of our questions and stated that his role in coordinating this type of assistance in Russia is nonexistent because DOE, through its SLD-Core program, conducts and coordinates radiation detection assistance provided to Russia. Lastly, we interviewed the advisor responsible for overseeing implementation of U.S. assistance to the Republic of Georgia because Georgia has received radiation detection equipment in the past from multiple U.S. programs. To obtain responses to our structured interview questions, we generally used e-mail and phone interviews. However, during our visits to Georgia and Ukraine, we were able to meet with the in-country advisors to obtain responses to our questions.

To assess the current and expected future costs of U.S. programs that provide radiation detection equipment assistance to foreign countries, we reviewed documents from DOE, DOD, State, and DHS detailing program expenditures, projected costs, and schedule estimates. We reviewed contract data for expenditures through the end of fiscal year 2005 and met numerous times with officials from DOE, DOD, State, and DHS to discuss the data. We obtained responses from key database officials to a number of questions focused on data reliability covering issues such as data entry access, internal control procedures, and the accuracy and completeness of the data. Follow-up questions were added whenever necessary. Caveats and limitations to the data were noted in the documentation where necessary. For example, in our discussions with the DOD official who manages its financial database, she stated that program support costs were prorated between WMD-PPI's projects based on usage. Therefore, the expenditure amount added for the program support cost for Uzbekistan is a reasonable approximation but may not be exact. We determined that the data we received were sufficiently reliable for the purposes of this report based on work we performed.

To identify challenges U.S. programs face in deploying and operating radiation detection equipment in foreign countries, we examined documents and spoke with officials from DOE, DOD, State, DHS, Los Alamos National Laboratory, Sandia National Laboratories, Washington Group International, and several nongovernmental entities, including the Transnational Crime and Corruption Center at American University. Additionally, during our visits to Georgia, Greece, Macedonia, Russia, Ukraine, and Uzbekistan we spoke with various foreign officials to better

understand the challenges they face in operating radiation detection equipment provided by U.S. programs. We also attended a National Academies of Science conference on nonintrusive technologies for improving the security of containerized maritime cargo and the National Cargo Security Council conference on radiation detection and screening.

To understand the steps U.S. programs take to coordinate radiation detection equipment assistance provided by multiple U.S. programs, we met with program officials from each of the agencies providing assistance and reviewed pertinent documents, including individual agency's assistance plans and State's *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas*. We also assessed coordination through the interagency group headed by State and met with the lead official of that effort—the Director of Export Control and Cooperation—and members of his staff. We discussed coordination issues with U.S. advisors stationed in countries receiving U.S. assistance including Armenia, Azerbaijan, Georgia, Kazakhstan, Malta, Moldova, Poland, Romania, and Ukraine. Several of these advisors were responsible for tracking assistance efforts in more than one country. For example, the advisor stationed in Poland is also responsible for Estonia, Latvia, and Lithuania. Finally, we relied on our previous reviews of the U.S. nonproliferation programs within DOE, DOD, and State. At State, we interviewed the Coordinator of U.S. Assistance to Europe and Eurasia and met with officials from the Bureau of International Security and Nonproliferation. We also relied on related prior GAO reports. We performed our review from April 2005 to February 2006 in accordance with generally accepted government auditing standards.

Appendix II

Additional Information on Radiation Detection Assistance Programs at the Department of Energy

The Department of Energy's (DOE) Second Line of Defense "Core" program provides comprehensive radiation detection equipment packages to foreign countries to combat nuclear smuggling. Its associated maintenance program focuses on maintaining equipment previously provided by the Department of State and other U.S. agencies. In addition, DOE implements another program within its Office of Global Threat Reduction that provides handheld radiation detection equipment to foreign countries.

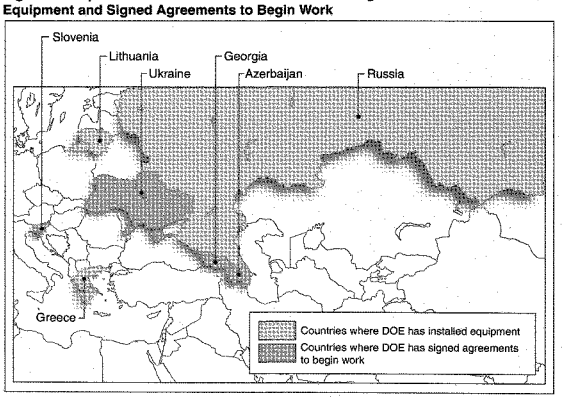
Second Line of Defense "Core" Program

In 1998, DOE established the Second Line of Defense "Core" (SLD-Core) program, which has primarily worked to help Russia detect illicit nuclear materials trafficking by providing radiation detection equipment to the Federal Customs Service of Russia. DOE recently expanded its efforts in the SLD-Core program to include countries other than Russia. SLD-Core activities focus on providing radiation detection equipment, software and hardware communications equipment and support, and training/processes to foreign countries' border sites. The radiation detection equipment DOE provides is U.S.-made, except in Russia where Russian-made equipment is installed. The communication systems DOE installs provide important information on the radiation detector alarms, such as the radiation profile of the substance detected. In addition to training at sites where equipment is installed, DOE provides other training courses at the Hazardous Materials Management and Emergency Response training center at Pacific Northwest National Laboratory.

Through the end of fiscal year 2005, DOE's SLD-Core program had completed installation of radiation portal monitors at 83 sites in Greece, Lithuania, and Russia at a cost of about $130 million. In fiscal year 2005, DOE planned to complete 29 sites in seven countries: Azerbaijan, Georgia, Kazakhstan, Russia, Slovenia, and Ukraine. However, due to delays in signing implementing agreements with the governments of some of these countries, many of these sites were not completed. As of December 2005, DOE had signed implementing agreements with Azerbaijan, Georgia, Slovenia, and Ukraine, and plans to commence work in these countries in fiscal year 2006 (see fig. 6). Additionally, the SLD-Core program will be installing radiation detection equipment at some foreign ports, referred to as "feeder" ports, to assist the work done by DOE's Megaports Initiative.[1]

[1]For more information on the Megaports Initiative, see GAO-05-375.

Figure 6: Map of Countries Where DOE's SLD-Core Program Has Installed Equipment and Signed Agreements to Begin Work



Source: DOE.

DOE has been cooperating with the Federal Customs Service of Russia since 1998, and, coupled with the large number of sites where Russia has installed equipment on its own, the nature of DOE's work through the SLD-Core program in Russia is evolving. DOE is transitioning its activities in Russia from installation of new equipment to sustainability of equipment it has previously installed. DOE and the Federal Customs Service of Russia signed an agreement in April 2005 that details plans for the long-term sustainability of radiation detection equipment DOE has provided to Russia. DOE is also now supporting other activities in Russia, such as regional radiation alarm response exercises and rechecks of previously installed equipment.

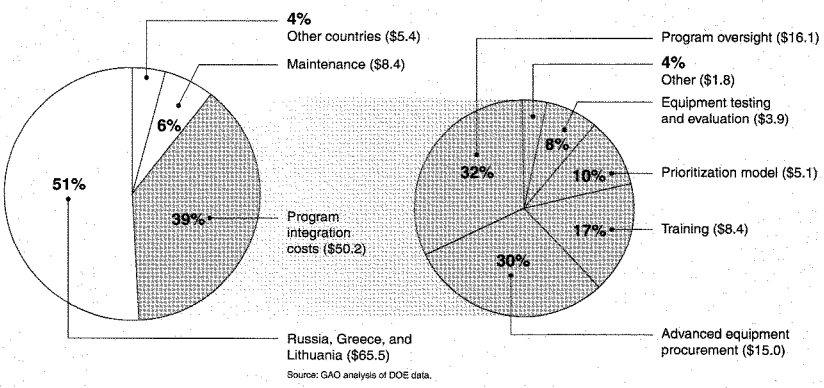
Through the end of fiscal year 2005, DOE spent about $66 million installing radiation portal monitors at 78 border sites in Russia, 4 sites in Greece, 1 site in Lithuania, and to conduct preliminary site assessments in other countries. DOE spent about $50 million on various program integration activities, which are costs not directly associated with installing equipment at a particular site within a specific country. Of this amount, about $15

million was spent on advanced equipment procurement activities, which include the purchase and storage of portal monitors and associated spare parts for use at future installations. DOE also spent almost $16 million on program oversight activities, such as program cost and schedule estimating, technical assistance provided by participating national laboratories, and translation services. In addition, DOE spent over $5 million to develop and maintain its prioritization model for the SLD-Core program, maintained by Los Alamos National Laboratory, which is used to rank foreign countries, as well as specific sites within a country, in terms of their attractiveness to a potential nuclear material smuggler. DOE also spent about $4 million on equipment testing and evaluation to test the effectiveness and performance of the radiation detection equipment that it provides through the program. DOE spent over $8 million on the development of materials and curricula for training foreign customs agents on the use of radiation detection equipment.[2] Finally, DOE spent almost $2 million on other program integration activities. See figure 7 for more information on program integration expenditures.

[2]Additionally, some of these funds were spent to pay for training of U.S. Customs and Border Protection officials at the Hazardous Materials Management and Emergency Response training center at Pacific Northwest National Laboratory.

Figure 7: DOE Spending on the SLD-Core Program through the End of Fiscal Year 2005

Dollars in millions



Source: GAO analysis of DOE data.

Note: Figures have been rounded.

DOE's Maintenance of Equipment Previously Installed by Other U.S. Agencies

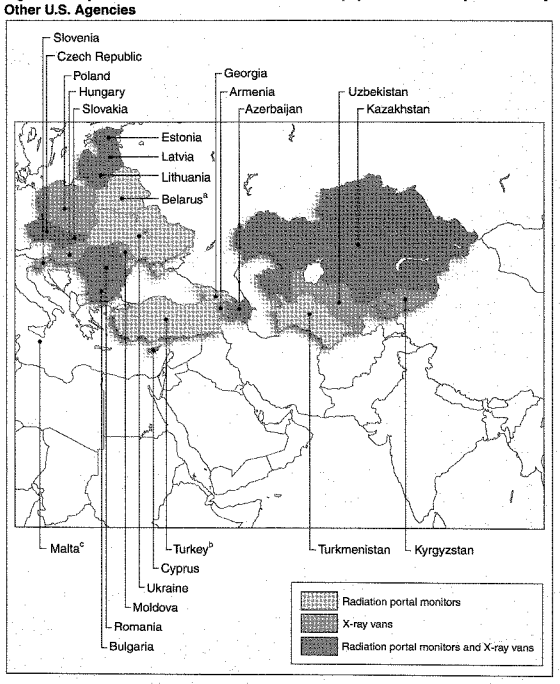
In 2002, DOE assumed the responsibility for maintaining certain radiation detection equipment, such as radiation portal monitors and X-ray vans with gamma radiation detection capability, previously installed in 23 countries by State and other U.S. agencies (see fig. 8). Through the end of fiscal year 2005, DOE has successfully conducted maintenance and sustainability activities for this equipment in 21 of 23 countries.[3] DOE contractors service these radiation portal monitors annually and X-ray vans biannually. Since 2002, DOE has spent about $8 million to provide spare parts, preventative

[3]DOE officials told us that, although Belarus has received a significant amount of radiation detection equipment from U.S. programs, it is currently prohibited from maintaining this equipment due to restrictions placed on U.S. assistance to Belarus through State's Selective Engagement Policy, which was instituted in 1997. Additionally, at the request of the government of Turkey, DOE no longer maintains radiation detection equipment provided to that country by State.

maintenance, and repairs for this equipment.[4] DOE anticipates that the future scope of the maintenance program will be reduced as the SLD-Core program expands into countries where equipment was previously installed by other U.S. agencies.

[4]State, through an interagency agreement with DOE, annually provides DOE with a portion of the funding required to maintain the equipment that State and other U.S. agencies previously installed. Through fiscal year 2005, State has provided DOE with approximately $3.2 million, which has been about one-third of the required funding necessary to conduct these activities. We have included these expenditures in the total expenditures for DOE's SLD-Core program.

Figure 8: Map of Countries Where DOE Maintains Equipment Previously Provided by Other U.S. Agencies



Source: DOE.

[a]DOE has not maintained equipment DOD provided to Belarus.

[b]At the request of the government of Turkey, DOE has not maintained equipment State provided to that country.

[c]State provided Malta with both radiation portal monitors and X-ray vans.

If DOE is notified that there are problems with the radiation portal monitors in a certain country, they will add this repair onto a scheduled maintenance trip of a nearby country. According to the DOE maintenance contractor, this occurs 5-6 times a year. However, DOE officials often are not made aware of specific problems with equipment prior to arriving at the site to conduct regular servicing. As a result, DOE's maintenance teams must be equipped with a wide variety of components in the event that major repairs are required. At times, maintenance teams have had to improvise temporary repairs for equipment due to a lack of necessary replacement parts. For example, during our visit to a border site in Ukraine, DOE's maintenance team discovered that a truck had struck and damaged a pole holding the wiring for the radiation detection equipment's communication systems. The truck's impact caused the wiring to snap in numerous places. Because the maintenance team was unaware of this damage prior to our arrival at the site, it had to repair the cable using connectors rather than replacing the entire wire as they would have preferred to do. DOE officials told us that, during the next scheduled maintenance visit to this site, the wiring will be replaced.

Cooperative Radiological Instrument Transfer Project

In 2004, DOE established the Cooperative Radiological Instrument Transfer project (CRITr) within its Global Threat Reduction Initiative.[5] In this project, DOE partners with Interpol, which provides knowledge of foreign law enforcement to determine the countries to select for assistance and coordinates all CRITr training logistics within its member countries.[6] Through the CRITr project, DOE collects and refurbishes handheld radiation detection devices deemed surplus by DOE national laboratories and provides this equipment to first responders in foreign countries. The handheld radiation detection equipment DOE provides through CRITr

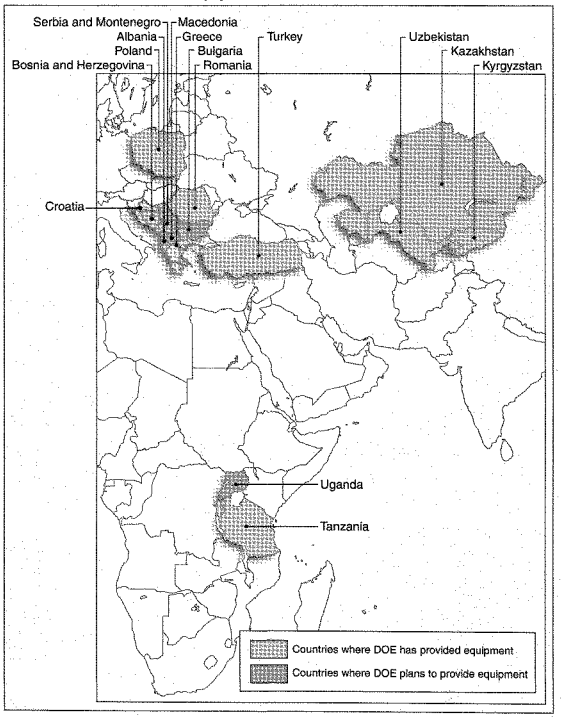
[5]The Global Threat Reduction Initiative consolidated DOE's efforts to identify, secure, remove, and/or facilitate disposition of high-risk nuclear and other radioactive materials around the world that pose a potential threat to the international community. Within this office, DOE's International Radiological Threat Reduction program works to locate, identify, recover, consolidate, and enhance the security of dangerous radioactive materials outside the United States.

[6]Interpol is the largest international police organization focusing on cross border police cooperation.

consists mostly of survey meters and does not include radiation pagers.[7] In addition to providing radiation detection equipment through the CRITr project, DOE provides training for foreign officials on how to use the equipment. DOE originally provided assistance through the CRITr project in Greece by providing over 100 handheld radiation detection devices prior to the Olympic Games in 2004. According to DOE officials, in fiscal year 2004, with Interpol's assistance, DOE selected seven additional countries to receive assistance through the project: Croatia, Kazakhstan, Kyrgyzstan, Poland, Romania, Turkey, and Uzbekistan (see fig. 9). DOE also provided radiation detection equipment to Tanzania in fiscal year 2005. Through the CRITr project, DOE spent almost $0.5 million in fiscal year 2004 and almost $0.6 million in fiscal year 2005, according to DOE officials. DOE has budgeted almost $0.4 million for fiscal year 2006 to supply instruments and training to law enforcement officials in Albania, Bosnia and Herzegovina, Bulgaria, Macedonia, Serbia and Montenegro, and Uganda and to provide additional equipment to Tanzania.

[7]In addition to the CRITr project, DOE's International Radiological Threat Reduction program has provided some radiation detection equipment to nuclear regulatory bodies and national laboratories in foreign countries. This equipment is intended to help these entities locate and identify orphaned radiological sources within their countries, rather than for law enforcement purposes. As a result, we did not include this part of DOE's radiation detection assistance in our review.

Figure 9: Map of Countries Where DOE's CRITr Project Has Provided and Plans to Provide Radiation Detection Equipment



Source: DOE.

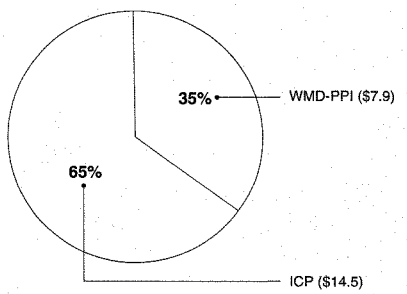
Appendix III

Additional Information on Radiation Detection Assistance Programs at the Department of Defense

The Department of Defense (DOD) implements two programs that assist other countries in combating nuclear smuggling: the Weapons of Mass Destruction Proliferation Prevention Initiative (WMD-PPI) and the International Counterproliferation Program (ICP). As figure 10 shows, DOD spent about $22 million on these programs between fiscal years 1994 and 2005.

Figure 10: DOD Spending on Radiation Detection Equipment Assistance Programs through the End of Fiscal Year 2005

Dollars in millions



Source: GAO analysis of DOD data.

Note: Figures have been rounded.

Weapons of Mass Destruction Proliferation Prevention Initiative

WMD-PPI was created as a project within the Cooperative Threat Reduction Program[1] and is implemented by DOD's Defense Threat Reduction Agency with oversight and policy guidance from the Office of

[1]Congress passed the Soviet Nuclear Threat Reduction Act of 1991, Pub. L. No. 102-228 (1991), popularly referred to as the Nunn-Lugar Act, authorizing U.S. threat reduction assistance to the former Soviet Union, due to concerns about the safety and security of Soviet nuclear weapons. The legislation authorized funding to assist the former Soviet Union with its efforts to (1) destroy nuclear, chemical, and other weapons; (2) transport, store, disable, and safeguard weapons in connection with their destruction; and (3) establish verifiable safeguards against the proliferation of such weapons.

the Undersecretary of Defense for Policy. In the 2003 National Defense Authorization Act, the Congress created WMD-PPI with a $40 million budget to prevent the proliferation of weapons of mass destruction (WMD) and related materials and technologies from the former Soviet Union.[2] WMD-PPI seeks to accomplish this mission through three projects: the Uzbekistan Land Border project, the Caspian Sea Maritime Proliferation Prevention project in Azerbaijan and Kazakhstan, and the Ukraine Land and Maritime Border projects.

- In Uzbekistan, DOD is installing radiation portal monitors at 17 sites; 11 of which were completed by the end of fiscal year 2005. To date, WMD-PPI has spent over $6 million to install radiation portal monitors in Uzbekistan. However, this spending total is misleading because DOD has obligated over $19 million to three contracts for program costs associated with installing radiation detection equipment, such as communication systems and training. Because DOD only executes spending on these contracts after all work has been completed, these contracts were not paid in fiscal year 2005. DOD projects that the Uzbekistan Portal Monitoring project will cost about $54 million and be completed in fiscal year 2009. Once these portal monitors are installed in fiscal year 2006, DOE will maintain the equipment within its Second Line of Defense "Core" program.

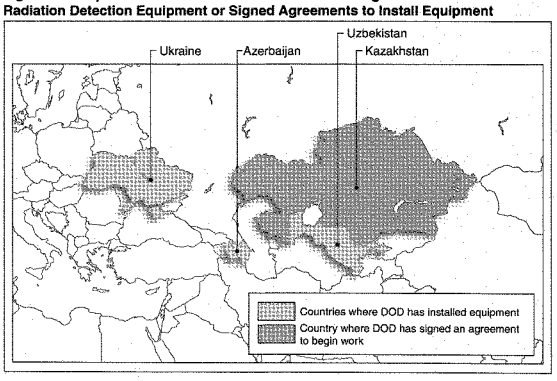
- The Caspian Sea project focuses on improving command and control, surveillance, detection and interception of WMD, operation, and sustainability along the Caspian Sea border by providing training and associated equipment, including handheld radiation detection devices. In Azerbaijan, the project's cost is estimated at $63.4 million and, in Kazakhstan, it is estimated at $60.6 million.

- In Ukraine, WMD-PPI is implementing a similar project along the Black Sea border. The Maritime Border Security Project in Ukraine is expected to cost over $39 million and will be finished in fiscal year 2009. The Ukrainian Land Border Forces Proliferation Prevention project focuses on securing the points of entry and the green border—border that is not a formal crossing point between countries—between Moldova and Ukraine. It seeks to improve Ukraine's capabilities to detect and interdict WMD and related materials by providing equipment and training. Radiation detection equipment, such as pagers, is included in

[2]Pub. L. No. 107-314 (2002).

this equipment assistance. DOD expects this project will cost over $51 million and be completed in fiscal year 2008.

Figure 11: Map of Countries Where DOD's WMD-PPI Program Has Provided Radiation Detection Equipment or Signed Agreements to Install Equipment



Source: DOD.

International Counterproliferation Program

The 1995 National Defense Authorization Act directed DOD and the Federal Bureau of Investigation to establish a program to improve efforts to deter the possible proliferation and acquisition of WMD and related materials across the borders and through the former Soviet Union, the Baltic region, and Eastern Europe.[3] Similarly, the 1997 National Defense Authorization Act directed DOD to work with U.S. Customs to carry out programs to assist customs officials and border guards in those regions in preventing unauthorized transfer and transportation of WMD and related materials.[4] DOD established ICP in response to these requirements. The

[3]Pub. L. No. 103-337 (1994).

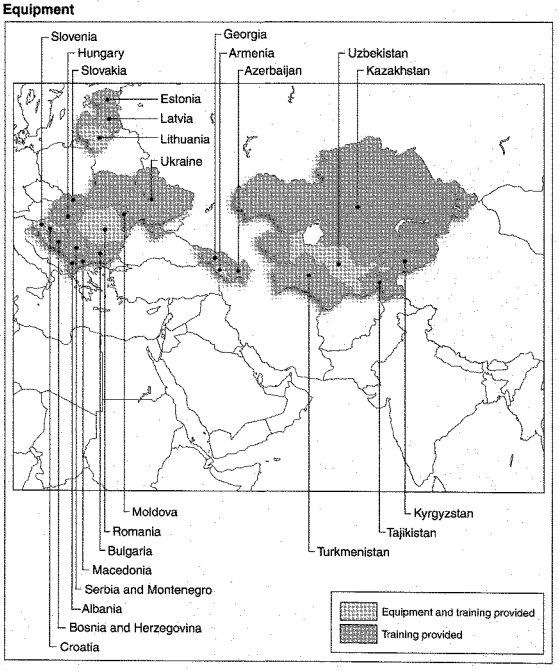
[4]Pub. L. No. 104-201 (1996).

program is implemented by the Defense Threat Reduction Agency. According to DOD officials, ICP policy guidance comes from DOD's Eurasia Department because of its strong ties and contacts within the regional scope of the program. Through ICP, DOD provides a range of law enforcement and border security training and equipment, including handheld radiation detection equipment, to foreign law enforcement officials in participating countries. According to an ICP official, the program does not currently provide much radiation detection equipment because, in many countries, other U.S. programs have already provided such equipment. ICP coordinates with the Federal Bureau of Investigation to conduct training of foreign government personnel. In some participating countries, ICP provides both equipment and training, and in others it provides only training, depending upon the needs of the country.

Through the end of fiscal year 2005, DOD had spent over $14 million to provide radiation detection equipment and radiation detection training to foreign countries through ICP. Of this amount, DOD spent over $0.5 million to provide handheld radiation detection equipment to six countries (see fig. 12). The remaining funds were spent on a variety of training related to radiation detection, WMD interdiction, and crime scene investigation.[5] Figure 13 shows the flowchart of training DOD provides to participating countries through ICP.

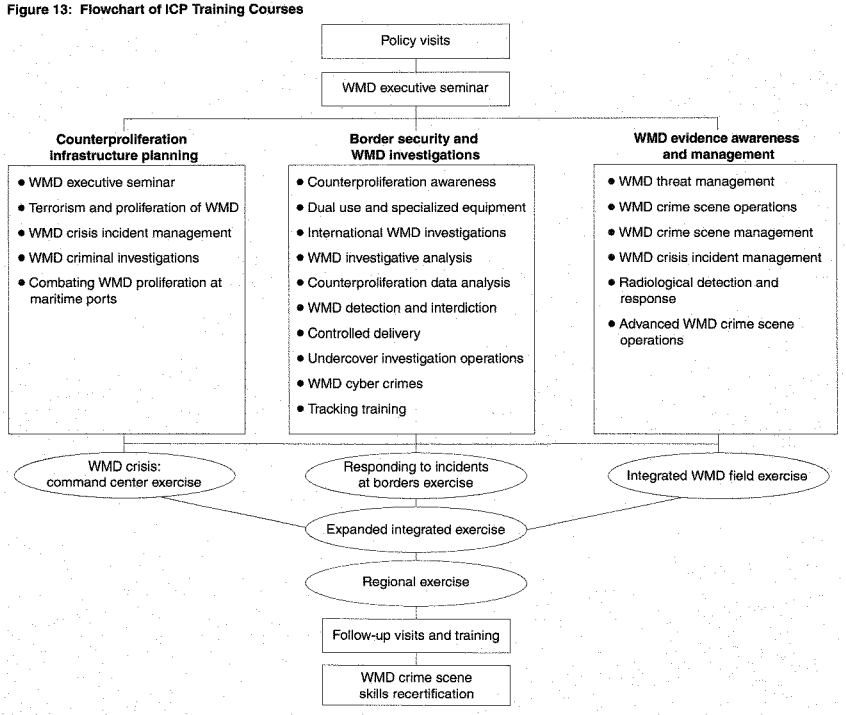
[5]Most ICP training courses do not focus solely on radiation detection training but have a module during the training on radiation detection. Therefore, according to a DOD official, breaking out the specific cost of radiation detection training is difficult. Only one ICP training course focuses solely on radiation detection.

Figure 12: Map of Countries Where DOD's ICP Has Provided Radiation Detection Equipment



Source: DOD.

Figure 13: Flowchart of ICP Training Courses



Source: DOD.

According to ICP officials, the program has worked in 23 countries, including Bosnia and Herzegovina, Bulgaria, Croatia, Serbia and Montenegro, Ukraine, and Uzbekistan. In the National Defense

Authorization Act of Fiscal Year 2005,[6] DOD was given permission by the Congress to expand ICP's scope outside of the original region. According to a DOD official, ICP plans to initiate programs in Malaysia, Singapore, and Pakistan.

[6]Pub. L. No. 108-375 (2004).

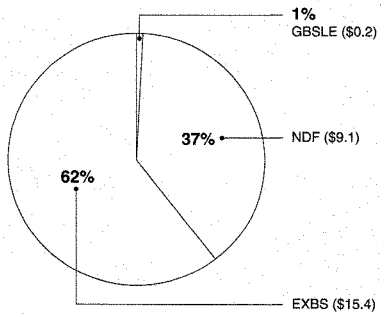
Appendix IV

Additional Information on Radiation Detection Assistance Programs at the Department of State

Since fiscal year 1994, the Department of State (State) has provided various types of radiation detection equipment assistance to 31 foreign countries. State has provided this assistance, primarily through three programs (1) the Export Control and Related Border Security program (EXBS), (2) the Nonproliferation and Disarmament Fund (NDF), and (3) the Georgia Border Security and Law Enforcement program (GBSLE). As figure 14 shows, State spent about $25 million from fiscal year 1994 through fiscal year 2005 on radiation detection equipment assistance to foreign countries.

Figure 14: State Spending on Radiation Detection Equipment Assistance Programs through the End of Fiscal Year 2005

Dollars in millions



Source: GAO analysis of State data.

Note: Figures have been rounded.

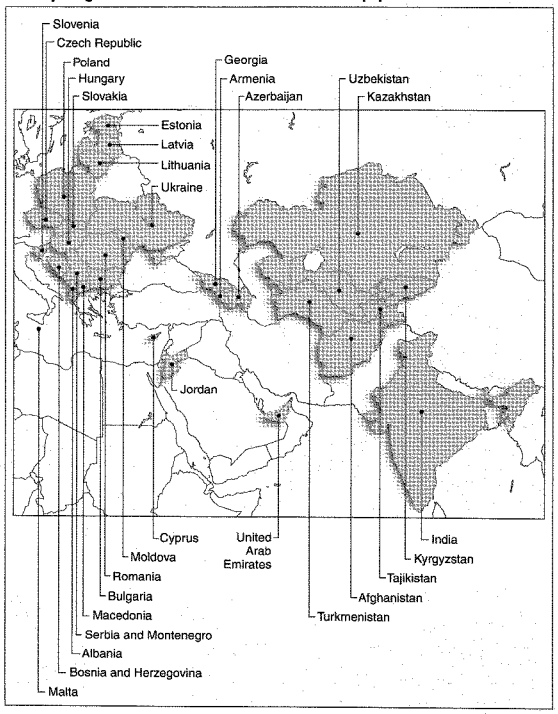
Export Control and Related Border Security Program

State's Export Control and Related Border Security program, which began in 1998, is a comprehensive U.S. government effort to help foreign countries improve their export controls and border security capabilities.[1] The program provides a broad array of assistance to foreign countries, such as workshops to assist foreign countries draft and implement new export control laws and regulations, as well as various types of equipment and training for foreign border control agencies. Assistance provided through the program focuses on five core areas: (1) laws and regulations, (2) licensing, (3) enforcement, (4) government and industry cooperation, and (5) interagency cooperation and coordination. While the original focus of the program was to provide assistance to potential "source countries" in the former Soviet Union or to countries that produce munitions or dual-use items,[2] State later expanded the program's focus to include states on potential smuggling routes in Eastern and Central Europe, East Asia, Central Asia, the Caucasus, Latin America, and Africa, as well as potential "source countries" in South Asia and countries with major transshipment hubs in the Mediterranean, Middle East, and Southeast Asia. Through the end of fiscal year 2005, State has spent $15.4 million to provide a variety of radiation detection equipment assistance to 30 countries (see fig. 15).

[1]State's Bureau of International Security and Nonproliferation manages the Export Control and Related Border Security program. In 1998, an export control assistance account was established as part of the Nonproliferation, Anti-terrorism, De-Mining and Related Programs account of the Foreign Operations Appropriations Act. Pub. L. No. 105-118 (1997). In fiscal year 2000, this program evolved into the Export Control and Related Border Security program.

[2]A "source country" is a country known to possess material that can be used to develop a weapon of mass destruction. For example, a country known to possess plutonium or highly enriched uranium would be considered a "source country."

Figure 15: Map of Countries Where State's Export Control and Related Border Security Program Has Provided Radiation Detection Equipment



Source: State.

In addition, State also provided funding to the Department of Homeland Security's (DHS) Customs and Border Protection (formerly known as U.S. Customs) to implement certain types of radiation detection equipment assistance on behalf of its Export Control and Related Border Security program. Specifically, from fiscal year 1999 through 2005, DHS and its predecessor organizations spent about $10.5 million to provide radiation detection equipment and training to 30 countries. This equipment included, among other things, radiation pagers that border officials wear on their belts and radioactive isotope identification devices. Training provided by DHS included assistance in operating the X-ray vans equipped with radiation detectors, hands-on instruction in using radiation detection equipment to detect nuclear smuggling, teaching techniques for investigating smuggling operations, and tracking the movements of smugglers between ports of entry. In addition, DHS also stationed 22 in-country advisors covering 25 countries, on behalf of the program, to assist in implementing and coordinating U.S. government assistance in these countries. In February 2005, State, through its EXBS program, assumed direct responsibility of the in-country advisors from DHS. According to State officials, this management change was done to better address coordination and responsiveness issues in the advisor program.

Russian Federal Customs Service Central Command Center

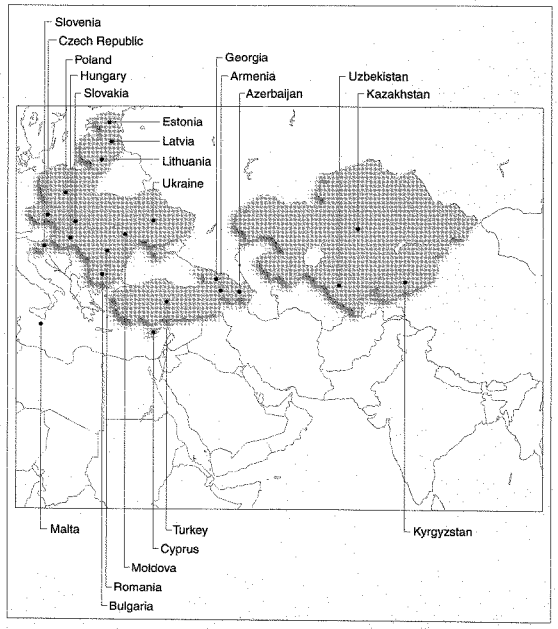
In addition to providing radiation detection equipment assistance to foreign countries, State has also provided other types of assistance designed to better ensure the effectiveness of radiation detection equipment previously provided to foreign countries through U.S. programs. Specifically, in fiscal year 2005, State, through its EXBS program, spent about $1.5 million to fund construction of a national command center for the Federal Customs Service of Russia. Through this project, portal monitors located at various Russian border sites can be directly linked to a national command center, located at Federal Customs Service headquarters in Moscow. By doing so, alarm data can be simultaneously evaluated by Russian officials both at the site and up the chain of command, thus establishing redundant layers of accountability for responding to alarms. For example, when a portal monitor alarms at a specific land border site, airport, or seaport, information will immediately be sent from the site directly to the command center enabling Russian officials to identify which specific site an alarm occurred at, quickly analyze it, and respond appropriately. Prior to the initiation of this project, the Federal Customs Service did not have an effective way to coordinate and integrate all of the information at its borders. While the total scope of work to be done at the command center has not been clearly defined yet, State officials told us that the primary activity will be to maintain and respond to alarm data from the various

border sites. State officials we spoke with stated that linking alarm data from the local alarm station at individual border sites to a centrally located command center will enhance Russia's ability to (1) ensure that U.S. provided equipment is being properly operated, (2) mitigate the possibility of corruption or other nefarious acts being committed by its border guards, and (3) effectively respond to any alarms and/or seizures of illicitly trafficked nuclear or radiological materials.

Nonproliferation and Disarmament Fund

State's Nonproliferation and Disarmament Fund spent approximately $9.1 million, from fiscal year 1994 through 2001, to provide various types of radiation detection equipment assistance to 21 countries (see fig. 16). This assistance included vehicle portal monitors, mobile vans equipped with X-ray machines and radiation detection equipment, handheld radiation detectors, dosimeters, and radiation pagers. For example, in fiscal year 2001, State approved a $1.3 million NDF project to install vehicle portal monitors at 16 sites in one country, and a $0.5 million project to assist another country's upgrading its domestically produced portal monitors in order to better detect nuclear material. State also provided $0.8 million to DHS to provide radiation detection equipment and training to seven countries under a project called "Project Amber." Of this amount, DHS spent $0.6 million to implement the project in these countries. In fiscal year 2001, State began to consolidate its assistance provided to foreign countries for the purposes of combating nuclear smuggling under its EXBS program. However, State officials told us that they have not yet determined whether or not they will fund any future projects to provide radiation detection equipment to foreign countries through NDF. As a result, it is uncertain how many other projects State will fund through NDF, in what countries these projects will be conducted, or how much they will cost.

Figure 16: Map of Countries Where State's Nonproliferation and Disarmament Fund Has Provided Radiation Detection Equipment



Source: State.

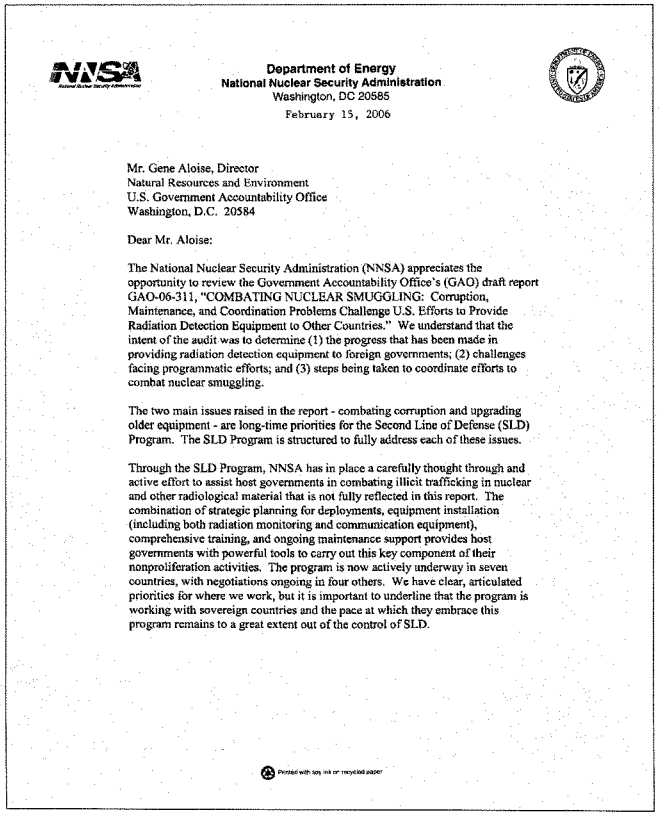
Georgia Border Security and Law Enforcement Program

State's Georgia Border Security and Law Enforcement program focuses on developing the Republic of Georgia's border infrastructure by assisting the Georgian Customs Administration and Georgian Border Guards in gaining control of the country's borders and seacoast and strengthening its border

security against any type of crime. The program primarily focuses on establishing a transparent land border regime with Azerbaijan, Armenia, and Turkey and strengthening border security against nuclear smuggling. As such, the program has provided assistance to enhance the Georgian Border Guards' capabilities to prevent, deter, and detect potential weapons of mass destruction smuggling. Through the program, State has provided a limited amount of radiation detection equipment assistance. Specifically, in fiscal year 1999, State spent $0.2 million to provide 137 radiation detection pagers to Georgia. According to State officials, no radiation detection equipment has been provided through the program since fiscal year 1999. However, State officials also told us that they have not yet determined if they will provide any additional radiation detection equipment assistance through the program to the Republic of Georgia in the future. As a result, it is uncertain what additional equipment State might provide or how much it will cost.

Appendix V

Comments from the Department of Energy



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

February 15, 2006

Mr. Gene Aloise, Director
Natural Resources and Environment
U.S. Government Accountability Office
Washington, D.C. 20584

Dear Mr. Aloise:

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report GAO-06-311, "COMBATING NUCLEAR SMUGGLING: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries." We understand that the intent of the audit was to determine (1) the progress that has been made in providing radiation detection equipment to foreign governments; (2) challenges facing programmatic efforts; and (3) steps being taken to coordinate efforts to combat nuclear smuggling.

The two main issues raised in the report - combating corruption and upgrading older equipment - are long-time priorities for the Second Line of Defense (SLD) Program. The SLD Program is structured to fully address each of these issues.

Through the SLD Program, NNSA has in place a carefully thought through and active effort to assist host governments in combating illicit trafficking in nuclear and other radiological material that is not fully reflected in this report. The combination of strategic planning for deployments, equipment installation (including both radiation monitoring and communication equipment), comprehensive training, and ongoing maintenance support provides host governments with powerful tools to carry out this key component of their nonproliferation activities. The program is now actively underway in seven countries, with negotiations ongoing in four others. We have clear, articulated priorities for where we work, but it is important to underline that the program is working with sovereign countries and the pace at which they embrace this program remains to a great extent out of the control of SLD.

Printed with soy ink on recycled paper

The SLD programs addresses corruption by requiring that all radiation portal monitors deployed under the program be networked to at least one central alarm station. The associated communications software requires reporting by a host country operator on the cause of the alarm and a summary of the actions taken in response to the alarm. Installations and operations are structured so that more than one person will be involved in reviewing and closing an alarm, thus making it more difficult for a corrupt official to bypass the system. One reason the program does not like single monitor installations – without communications systems, without full site coverage, and without high level support – is that these types of systems are the most vulnerable to corruption. Additionally, SLD planning includes redundant monitors (on both sides of a border) along key pathways to protect against corruption at a single site. In certain countries, the SLD Program will provide the means to send status of health, alarm and other data to central locations within the host country for further oversight and technical assistance. Such systems are under development in Russia and are being deployed in Greece. Based on these experiences, the program will deploy these systems more widely. We have established a methodology for selecting those countries in which the systems will be installed and will ensure that our fiscal planning documents reflect this approach. Programs that help ensure personnel reliability are under consideration for selected countries. We do not believe that the cost of such programs will considerably impact our life-cycle projections.

As to upgrading less sophisticated portal monitors previously installed by other U.S. agencies, we intend to replace these single monitors with full installations as part of our comprehensive country-wide program. In fact, to accelerate this process, we have significantly increased our Fiscal Year (FY) 2007 SLD Core activities Congressional Budget request. We firmly believe that upgrading single monitor installations, except in special circumstances, is not the best use of our resources. Such installations are more likely to be bypassed, to be vulnerable to corruption, and to fall into disuse or misuse because there is no training or sustainability program in place.

Finally, in response to the point made in the report that NNSA has not systematically maintained handheld radiation detection equipment provided by State and other agencies, we believe that the report does not adequately reflect what we have done in this area. We wish to clarify that the SLD maintenance program does in fact have a process in place to identify and replace non-functioning handheld equipment. SLD maintenance teams routinely inquire about the handhelds when performing regular maintenance of portal monitors. Maintenance of handheld equipment is provided whenever possible and units are being replaced on a case-by-case basis. In FY05, NNSA received reports from the maintenance teams that many sites were in need of additional or replacement

handheld detection equipment. In response, we ordered handhelds specifically for this purpose (135 units at a total cost of $386K). These units are being distributed to sites during the FY06 maintenance visits.

NNSA appreciates the efforts of GAO to incorporate changes to the original draft report. These changes clarify issues that are directly related to NNSA. We agree with the recommendations that are contained in the modified draft report and have enclosed our specific comments to those recommendations.

Should you have any questions related to this response, please contact Richard Speidel, NNSA's Director, Policy and Internal Controls Management.

Sincerely,

Michael C. Kane
Associate Administrator
for Management and Administration

Enclosure

cc: Deputy Administrator for Defense Nuclear Nonproliferation
Senior Procurement Executive
Director, Service Center

Comments to
GAO Draft Report, GAO-06-311
"COMBATING NUCLEAR SMUGGLING:
Corruption, Maintenance, and Coordination Problems
Challenge U.S. Efforts to Provide Radiation Detection
Equipment to Other Countries"

Recommendation 1

Integrate projected spending on specific anticorruption measures into the long-term cost estimates for the SLD-Core program.

Management Comment

Concur

NNSA has accomplished a significant portion of this work. We will factor cost estimates for centralized communications systems and personnel reliability programs. Since this is an ongoing effort we believe that NNSA has met the intent of the recommendation.

Recommendation 2

Upgrade less sophisticated portal monitors previously installed by other U.S. agencies where DOE has determined this to be appropriate as soon as possible and include funding to accomplish this in DOE's planning and budgeting process.

Management Comment

Concur

NNSA's plans and programs to upgrade these monitors in full-site installations as part of a country-wide program are captured within NNSA's Planning, Programming, Budgeting and Evaluation process. As such, the funding has been requested to accelerate this process. NNSA believes that we are responsive to the recommendation and have met its intent.

Appendix VI

Comments from the Department of State

United States Department of State
Washington, D.C. 20520

OCT 10 2006

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "COMBATING NUCLEAR SMUGGLING: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries," GAO Job Code 360560.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Keith Peterson, Diplomacy Officer, Bureau of International Security and Nonproliferation, at (202) 647-8629.

Sincerely,

Sid Kaplan (Acting)

cc: GAO – Stockton Butler
ISN – Donald Mahley
State/OIG – Mark Duda

Department of State Comments on the GAO Draft Report
COMBATING NUCLEAR SMUGGLING: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries
(GAO-06-311, GAO Code 360560)

In general, the Department of State concurs with the recommendations and conclusions contained in this report. The Department continues to refine U.S. government efforts to repair and maintain radiation detection equipment where such efforts are cost-effective to do so; agrees that updating the *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* with significant input from the National Nuclear Security Administration (NNSA) and other interagency partners would be beneficial; and continues to move forward in creating a comprehensive list of radiation detection equipment provided by the U.S. government overseas. The GAO rightly points to the interagency working groups chaired by the Department as a formal coordinating mechanism, but misses entirely the daily and informal coordinating role played by the Department's front-line country program officers in developing interagency program plans for their countries. The Department would like to emphasize that the primary means of coordination of its efforts concerning radiation detection equipment provision is at the action officer level via interagency contacts and not in formal meetings. It is clear from the evidence provided in this GAO report that the Department's action officers and their interagency and government contractor counterparts have done excellent work coordinating this effort in most areas.

The Department ensures the maintenance of radiation portal monitors based on a Memorandum of Understanding (MOU) with NNSA that stipulates that NNSA will provide repairs and maintenance to all radiation portal monitors provided by the Export Control and Related Border Security (EXBS) and other State programs. The Department is also engaged in ongoing discussions about the upgrading and replacement of obsolescent portal monitors provided in the past by the Department, and concurs with GAO's recommendation in this regard. The Department also has kept abreast of the similar MOU between NNSA and the Department of Defense on the maintenance of portal monitors noted in the GAO report. The Office of Export Control Cooperation (ECC) has during the course of the research and drafting of this report informed GAO of its efforts to develop a maintenance

Department of State Comments on the GAO Draft Report
COMBATING NUCLEAR SMUGGLING: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries
(GAO-06-311, GAO Code 360560)

In general, the Department of State concurs with the recommendations and conclusions contained in this report. The Department continues to refine U.S. government efforts to repair and maintain radiation detection equipment where such efforts are cost-effective to do so; agrees that updating the *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* with significant input from the National Nuclear Security Administration (NNSA) and other interagency partners would be beneficial; and continues to move forward in creating a comprehensive list of radiation detection equipment provided by the U.S. government overseas. The GAO rightly points to the interagency working groups chaired by the Department as a formal coordinating mechanism, but misses entirely the daily and informal coordinating role played by the Department's front-line country program officers in developing interagency program plans for their countries. The Department would like to emphasize that the primary means of coordination of its efforts concerning radiation detection equipment provision is at the action officer level via interagency contacts and not in formal meetings. It is clear from the evidence provided in this GAO report that the Department's action officers and their interagency and government contractor counterparts have done excellent work coordinating this effort in most areas.

The Department ensures the maintenance of radiation portal monitors based on a Memorandum of Understanding (MOU) with NNSA that stipulates that NNSA will provide repairs and maintenance to all radiation portal monitors provided by the Export Control and Related Border Security (EXBS) and other State programs. The Department is also engaged in ongoing discussions about the upgrading and replacement of obsolescent portal monitors provided in the past by the Department, and concurs with GAO's recommendation in this regard. The Department also has kept abreast of the similar MOU between NNSA and the Department of Defense on the maintenance of portal monitors noted in the GAO report. The Office of Export Control Cooperation (ECC) has during the course of the research and drafting of this report informed GAO of its efforts to develop a maintenance

countries, but the Advisors have competing claims on their time, many responsibilities within the program, and limited resources at their disposal. The Department has taken significant steps to strengthen both inventory and maintenance issues recommended by GAO since State assumed direct management of the Advisors program in February 2005. However, the complexity of the inventory and maintenance issue, which includes a vast amount of non-radiation detection equipment, is one with which the Department continues to grapple.

The Department does not concur with the statements and conclusions reached in the section entitled "State Coordinates U.S. Radiation Detection Equipment Assistance Through an Interagency Working Group and In-Country Advisors" because it is incomplete and does not reflect information provided by the Department to GAO in its communication of August 3, 2005 and in personal interviews. In those communications and interviews, the Department indicated that in the provision of radiation detection equipment, various mechanisms are used: the interagency working group, input from Advisors, and also consultations between ECC Country Officers and their interagency counterparts. The Department considers the last element to be the "primary coordination mechanism," rather than the interagency working group as asserted by GAO, because Country Officer interaction with their counterparts at NNSA, CBP, and DoD allow State to coordinate activities on a daily, informal, basis. The current GAO report provides many examples of in-depth, informal, daily coordination that has resulted in successful nonproliferation efforts in the area of provision of radiation detection equipment: a layered approach coordinated between State and NNSA in portal monitor deployment in Armenia and Georgia that accounts for the perceived corruption problems also noted by GAO, exemplifies the advantages of State's flexibility in providing radiation portal monitors when NNSA has trouble getting an agreement in place with the foreign government, and the ability of the EXBS program to move to address threats posed by proliferation networks (see footnote 6 in the GAO report). Another example that GAO provides is the intense coordination and daily activity by Country Officers that made possible the Russian Federal Customs Service Central Command Center, where NNSA provided the portal monitors and landlines to connect to the Center, while EXBS provided many of the other resources necessary to make the Center operational in ways that have the advantages noted in the GAO report. Such coordination, it is worth emphasizing, is intense, daily, and within the scope of the EXBS program, is

much more important that coordination with the interagency working group and/or with the in-country advisors.

The Department believes that substantial progress has been made over the last year in the provision of and coordination of radiation detection equipment. As noted in the GAO report, various providers of equipment and training do work together to create synergies that are important to the success of the mission of the EXBS and other programs. Since assuming management responsibility of the EXBS Advisors program, the Department has made important changes to address some of the concerns expressed in this report, such as requiring Advisors to perform end-use monitoring on specific equipment, including radiation detection equipment. The Department is near completion of a mechanism that will help EXBS better manage the various inventory and maintenance issues, and will revise the *Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas* with our interagency partners. Finally, the Department supports a multi-faceted approach to radiation monitoring, where both equipment provision and cutting edge training is performed while taking into consideration the diverse conditions, levels of technical capacity, and different threat profile posed by the countries in the EXBS program.

Related GAO Products

Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain. GAO-06-389. Washington, D.C.: March 14, 2006.

Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and in Other Countries. GAO-05-840T. Washington, D.C.: June 21, 2005.

Olympic Security: U.S. Support to Athens Games Provides Lessons for Future Olympics. GAO-05-547. Washington, D.C.: May 31, 2005.

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. GAO-05-375. Washington, D.C.: March 31, 2005.

Weapons of Mass Destruction: Nonproliferation Programs Need Better Integration. GAO-05-157. Washington, D.C.: January 28, 2005.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling. GAO-02-989T. Washington, D.C.: July 30, 2002.

Nuclear Nonproliferation: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning. GAO-02-426. Washington, D.C.: May 16, 2002.

United States Government Accountability Office

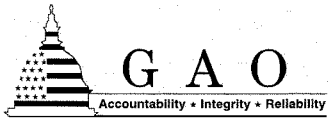
GAO

Report to Congressional Requesters

March 2006

COMBATING NUCLEAR SMUGGLING

DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain



GAO-06-389

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-389, a report to congressional requesters

March 2006

COMBATING NUCLEAR SMUGGLING

DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain

Why GAO Did This Study

Preventing radioactive material from being smuggled into the United States is a key national security objective. To help address this threat, in October 2002, DHS began deploying radiation detection equipment at U.S. ports-of-entry. This report reviews recent progress DHS has made (1) deploying radiation detection equipment, (2) using radiation detection equipment, (3) improving the capabilities and testing of this equipment, and (4) increasing cooperation between DHS and other federal agencies in conducting radiation detection programs.

What GAO Recommends

The Secretary of Homeland Security should work with other agencies, as necessary, to (1) streamline internal review procedures so that spending data can be provided to the Congress in a more timely way; (2) update the current deployment plan; (3) analyze the benefits and costs of advanced portals, then revise the program's cost estimates to reflect current decisions; (4) develop ways to effectively screen rail containers; (5) revise agency procedures for container inspection; and (6) develop a way for CBP officers to verify NRC licenses.

In commenting on a draft of this report, DHS stated that it agreed with, and will implement, our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-389.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gene Aloise, (202) 512-3841.

What GAO Found

The Department of Homeland Security (DHS) has made progress in deploying radiation detection equipment at U.S. ports-of-entry, but the agency's program goals are unrealistic and the program cost estimate is uncertain. As of December 2005, DHS had deployed 670 portal monitors and over 19,000 pieces of handheld radiation detection equipment. However, the deployment of portal monitors has fallen behind schedule, making DHS's goal of deploying 3,034 by September 2009 unlikely. In particular, two factors have contributed to the schedule delay. First, DHS provides the Congress with information on portal monitor acquisitions and deployments before releasing any funds. However, DHS's lengthy review process has caused delays in providing such information to the Congress. Second, difficult negotiations with seaport operators about placement of portal monitors and how to most efficiently screen rail cars have delayed deployments at seaports. Regarding the uncertainty of the program's cost estimate, DHS would like to deploy advanced technology portals that will likely cost significantly more than the currently deployed portals, but tests have not yet shown that these portals are demonstrably more effective than the current portals. Consequently, it is not clear that the benefits of the new portals would be worth any increased cost to the program. Also, our analysis of the program's costs indicates that DHS may incur a $342 million cost overrun.

DHS has improved in using detection equipment and in following the agency's inspection procedures since 2003, but we identified two potential issues in Customs and Border Protection (CBP) inspection procedures. First, although radiological materials being transported into the United States are generally required to have a Nuclear Regulatory Commission (NRC) license, regulations do not require that the license accompany the shipment. Further, CBP officers do not have access to data that could be used to verify that shippers have acquired the necessary documentation. Second, CBP inspection procedures do not require officers to open containers and inspect them, although under some circumstances, doing so could improve security. In addition, DHS has sponsored research, development, and testing activities to address the inherent limitations of currently fielded equipment. However, much work remains to achieve consistently better detection capabilities.

DHS seems to have made progress in coordinating with other agencies to conduct radiation detection programs; however, because the DHS office created to achieve the coordination is less than 1 year old, its working relationships with other agencies are in their early stages of development and implementation. In the future, this office plans to develop a "global architecture" to integrate several agencies' radiation detection efforts, including several international programs.

Contents

Abbreviations

ANSI	American National Standards Institute
CBP	Customs and Border Protection
CMTB	Counter Measures Test Bed
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOD	Department of Defense
DOE	Department of Energy
FBI	Federal Bureau of Investigation
FLETC	Federal Law Enforcement Training Center
GAO	Government Accountability Office
LSS	Laboratories and Scientific Services
NIST	National Institute for Standards and Technology
NTS	Nevada Test Site
NRC	Nuclear Regulatory Commission
PNNL	Pacific Northwest National Laboratory
S&T	DHS Science and Technology Directorate
TSA	Transportation Security Administration

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

March 22, 2006

Congressional Requesters

Since the attacks of September 11, 2001, combating terrorism has been one of the nation's highest priorities. As part of that effort, preventing radioactive material from being smuggled into the United States—perhaps to be used by terrorists in a nuclear weapon or in a radiological dispersal device (a "dirty bomb")—has become a key national security objective. The Department of Homeland Security (DHS) is responsible for providing radiation detection capabilities at U.S. ports-of-entry.[1] Until April 2005, U.S. Customs and Border Protection (CBP) managed this program. However, on April 15, 2005, the president directed the establishment, within DHS, of the Domestic Nuclear Detection Office (DNDO), whose duties include acquiring and supporting the deployment of radiation detection equipment.[2] CBP continues its traditional screening function at ports-of-entry to prevent illegal immigration and to interdict contraband, including the operation of radiation detection equipment. The Pacific Northwest National Laboratory (PNNL), one of the Department of Energy's (DOE) national laboratories, manages the deployment of radiation detection equipment for DHS.[3]

DHS's program to deploy radiation detection equipment at U.S. ports-of-entry has two goals. The first is to use this equipment to screen all cargo, vehicles, and individuals coming into the United States. The United States has over 380 border sites at which DHS plans to deploy radiation detection equipment. The volume of traffic entering the United States also adds to the size and complexity of the job. For example, each day, DHS processes about 64,000 containers arriving in the United States via ships, trucks, and

[1]The Departments of Energy, Defense, and State are also implementing programs to combat nuclear smuggling in other countries by providing radiation detection equipment and training to foreign border security personnel. See Pub. L. No. 107-296 (2002) Title IV, § 402. We recently reported on these programs in *Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries*, GAO-06-311 (Washington, D.C.: Mar. 14, 2006).

[2]See National Security Presidential Directive 43/Homeland Security Presidential Directive 14, Domestic Nuclear Detection (April 15, 2005).

[3]DOE manages the largest laboratory system of its kind in the world. The mission of DOE's 22 laboratories has evolved. Originally created to design and build atomic weapons, these laboratories have since expanded to conduct research in many disciplines—from high-energy physics to advanced computing.

rail cars; 365,000 vehicles; and more than 1.1 million people. The second goal of the program is to screen all of this traffic without delaying its movement into the nation. To illustrate the difficulty of achieving this second goal, CBP's port director at the San Ysidro, California, land border crossing estimated that prior to initiating radiation screening, the volume of traffic through the port-of-entry was so great that, at times, the wait to enter the United States from Mexico was about 2.5 hours. He noted that had radiation detection screening added a mere 20 seconds to the wait of each vehicle, the wait during those peak times could have increased to about 3.5 or 4 hours—an unacceptable outcome in his view. DHS's current plans call for completing deployments of radiation detection equipment at U.S. ports-of-entry by September 2009.

To screen commerce for radiation, CBP uses several types of detection equipment and a system of standard operating procedures. Current detection equipment includes radiation portal monitors, which can detect gamma radiation (emitted by all of the materials of greatest concern) and neutrons (emitted by only a limited number of materials, including plutonium—a material that can be used to make a nuclear weapon). CBP officers also carry personal radiation detectors—commonly referred to as "pagers"—small handheld devices that detect gamma radiation, but not neutrons. For the most part, pagers are meant to be personal safety devices, although they are used in some locations to assist with inspections. Finally, CBP officers also use radioactive isotope identification devices, which are handheld devices designed to determine the identity of radioactive material—that is, whether it is a nuclear material used in medicine or industry, a naturally occurring source of radiation, or weapons-grade material. All of these devices have limitations in their ability to detect and identify nuclear material.

Generally, CBP's standard procedures direct vehicles, containers, and people coming into the country to pass through portal monitors to screen for the presence of radiation. This "primary inspection" serves to alert CBP officers that a radioactive threat might be present. All traffic that causes an alarm during primary inspection is to undergo a "secondary inspection" that consists of screening with another portal monitor to confirm the presence of radiation, and includes CBP officers using radiation isotope identification devices to determine the source of radiation being emitted, (e.g., harmless sources, such as ceramics, or dangerous sources, such as weapons-grade nuclear material). If CBP officers identify a nuclear or radiological threat during a secondary inspection, or if the officers' pagers register a dangerously high level of radiation, then officers are to establish

a safe perimeter around the nuclear material and contact scientists in CBP's Laboratories and Scientific Services (LSS) for further guidance.[4] In some cases, CBP identifies incoming sea-bound cargo containers through a system that targets some containers for inspection based on their perceived level of risk. In these situations, CBP works with seaport terminals to have containers moved to an agreed-upon location for inspection. These inspections include the use of active imaging, such as an x-ray, and passive radiation detection, such as a radiation isotope identification device. Typically, if CBP officers find irregularities, physical examinations are conducted.

In September 2003, we reported on CBP's progress in completing domestic deployments. In particular, we reported that certain aspects of CBP's installation and use of the equipment diminished its effectiveness and that coordination among agencies on long-term research issues was limited. Since the issuance of our 2003 report, questions have arisen about the efficacy of the detection equipment CBP has deployed—in particular, its purported inability to distinguish naturally occurring radioactive materials from a nuclear bomb.

Because of the complexity and importance of these issues, you asked us to assess the progress made in (1) deploying radiation detection equipment at U.S. ports-of-entry and any problems associated with that deployment, (2) using radiation detection equipment at U.S. ports-of-entry and any problems associated with that use, (3) improving the capabilities and testing of this equipment, and (4) increasing the level of cooperation between DHS and other federal agencies in conducting radiation detection programs.

To address these objectives, we (1) analyzed CBP's project plan, including the project's costs and deployment schedules, to deploy radiation detection equipment at U.S. ports-of-entry; (2) visited several ports-of-entry, including two international mail and express courier facilities, five seaports, and three land border crossings; (3) participated in radiation detection training for CBP officers; and (4) visited four national laboratories, the Nevada Test Site, and an Air Force base involved with

[4]Laboratories and Scientific Services coordinates technical and scientific support to all CBP trade and border protection activities. These activities include, among other things, providing scientific/forensic support, including on-site support, to CBP officers and other government agencies with regard to the investigation and interdiction of Weapons of Mass Destruction.

testing and deploying radiation detection equipment. We focused primarily on the issues surrounding radiation portal monitors because they are a major tool in the federal government's efforts to thwart nuclear smuggling. We also focused on this equipment because its procurement and installation cost far exceeds the cost of procuring and deploying other radiation detection equipment such as handheld equipment also used at U.S. ports-of-entry. We reviewed documentation, such as deployment and cost figures, equipment test plans and results, and agency agreements to cooperate in detecting radiation. We also interviewed key program officials at each of these agencies to discuss the deployment of radiation detection equipment, attempts to improve the equipment's capabilities, and cooperation among agencies to protect the United States from nuclear terrorism. We performed a data reliability assessment of the data we received, and interviewed knowledgeable agency officials on the reliability of the data. We determined the data were sufficiently reliable for the purposes of this report. More details on our scope and methodology appear in appendix I. We conducted our review from March 2005 to February 2006 in accordance with generally accepted government auditing standards.

Results in Brief

Between October 2000 and October 2005, the United States spent about $286 million to deploy radiation detection equipment at domestic ports-of-entry. However, the deployment of portal monitors has fallen behind schedule, making DHS's goal of deploying 3,034 by 2009 unlikely. To meet its long-term goal, DHS would have to deploy about 52 portal monitors a month for the next 4 years—a rate that far exceeds the 2005 rate of about 22 per month. Moreover, the program's estimated total cost of $1.3 billion is highly uncertain. Several factors have contributed to the slow pace of deployment. First, program officials typically disburse funds to the contractor managing the deployment late in the fiscal year. For example, the contractor did not receive its fiscal year 2005 allocation until September 2005. These delays have caused the contractor to postpone or cancel contracts, sometimes delaying deployments. According to the House Appropriations Committee report on the CBP portion of DHS's fiscal year 2005 budget, CBP should provide the Congress with an acquisition and deployment plan for the portal monitor program prior to funding Pacific Northwest National Laboratory (PNNL). This plan took many months to finalize, mostly because it required multiple approvals within DHS and the Office of Management and Budget (OMB) prior to being submitted to the Congress. The lengthy review process delayed the release of funds and, in some cases, disrupted and delayed deployment. In fiscal year 2005, this process was further delayed by the creation of DNDO, and the uncertainty

regarding the new office's responsibilities. Second, negotiations with seaport operators to deploy portal monitors have taken longer than anticipated because some operators believe screening for radiation will adversely affect the flow of commerce through their ports. DHS has adopted a deployment policy designed to achieve cooperation with seaport operators because agency officials believe such arrangements are more efficient and, in the long term, probably more timely. Third, devising an effective way to conduct secondary inspections of rail traffic departing seaports without disrupting commerce has delayed deployments. This problem may worsen because the Department of Transportation (DOT) has forecast that the use of rail transit out of seaports will probably increase in the near future. Addressing and solving the problems with screening rail transport is critical to the successful completion of the DHS program.

Regarding the total cost of the project, CBP's $1.3 billion estimate is highly uncertain and overly optimistic. The estimate is based on CBP's plans for widespread deployment of advanced technology portal monitors currently being developed. However, the prototypes of this equipment have not yet been shown to be more effective than the portal monitors now in use, and DHS officials say they will not purchase the advanced portal monitors unless they are proven to be superior. Moreover, when the advanced technology portal monitors become commercially available, experts estimate that they will cost between about $330,000 and $460,000 each—far more than the currently-used portal monitors which cost between $49,000 and $60,000. The installation cost for both types of portal monitor is roughly $200,000. Even if future test results indicate better detection capabilities, without a detailed comparison of the two technologies' capabilities it is not clear that the dramatically higher cost for this new equipment would be worth the investment. Finally, our analysis of CBP's deployment data indicates that the program will probably experience a significant cost overrun of between $88 million and $596 million, with a $342 million overrun most likely.

The CBP officers we observed conducting primary and secondary inspections appeared to use radiation detection equipment correctly and to follow inspection procedures. In contrast, in 2003 we reported that CBP officers sometimes used radiation detection equipment in ways that reduced its effectiveness and sometimes did not follow agency procedures. Generally, CBP requires that its officers receive formal training in using radiation detection equipment, and many officers have gained experience and proficiency in using the equipment since the program's inception. However, we also identified two potential issues in CBP inspection

procedures that, if addressed, could strengthen the nation's defenses against nuclear smuggling. For example, individuals and organizations shipping radiological materials to the United States generally must acquire a Nuclear Regulatory Commission (NRC) license, but regulations do not require that the license accompany the shipment. Further, according to CBP officials, CBP officers lack access to NRC license data that could be used to verify that shippers of radiological material actually obtained required licenses, and to authenticate licenses that accompany shipments. The second potential issue pertains to CBP's guidance for conducting secondary inspections. Currently, CBP procedures require only that officers locate, isolate, and identify radiological material. Typically, officers perform an external examination by scanning the sides of cargo containers with a radiation isotope identification device during secondary inspections. The guidance does not specifically require officers to open containers and inspect their interiors, even when an external examination cannot unambiguously resolve an alarm. However, at one port-of-entry we visited, CBP officers routinely opened and entered commercial truck trailers to conduct secondary inspections when an external inspection could not locate and identify the radiological source. This approach increases the chances that the source of the radioactivity that originally set off the alarm will be correctly located and identified. According to senior CBP officials at this port-of-entry, this additional procedure has had little negative impact on the flow of commerce and has not increased the cost of CBP inspections, despite being implemented at one of the busiest commercial ports-of-entry in the nation.

DHS would like to improve the capabilities of currently-fielded radiation detection equipment. Today's equipment lacks a refined capability to rapidly determine the type of radioactive materials they detect, which means that CBP officers often conduct secondary inspections of containers carrying non-threatening material. To address this limitation, DHS has sponsored research, development, and testing activities that attempt to improve the capabilities of existing radiation portal monitors and to produce new, advanced technologies with even greater detection and identification enhancements. However, much work remains for the agency to achieve consistently better detection capabilities, as the efforts undertaken so far have had only mixed results. For example, DHS sponsored the development of a software package designed to reduce the number of false alarms from portal monitors already in widespread use. However, tests of the software have been largely inconclusive. In some test scenarios, there was little difference in detection capability between portal monitors equipped with—and without—the new software. Experts have

recommended further testing to improve the software's capabilities. Further, DHS is testing new, advanced portal monitors that use a technology designed to both detect the presence of radiation and identify its source. However, in tests performed during 2005, the detection capabilities of the advanced technology prototypes demonstrated mixed results—in some cases they worked better, but in other cases, they worked about the same as already deployed systems. In addition, DHS also sponsors a long-range research program aimed at developing innovative technologies designed to improve the capabilities of radiation detection equipment. For example, DHS is supporting research at two national laboratories on a new system designed to better detect radiation sources, even when shielded with materials designed to hide their presence. The two laboratories have constructed several prototypes, but currently the high cost of this technology limits its commercial attractiveness. Finally, DHS plans to use its new testing facility being built at the Nevada Test Site to improve on existing test capabilities and to support the agency's development, testing, acquisition, and deployment of radiation detection technologies.

Historically, cooperation between agencies conducting radiation detection programs has been limited. Currently DHS, largely through DNDO, cooperates with DOE, the Department of Defense (DOD), and other agencies to coordinate these programs; however, because DNDO was created less than 1 year ago, its cooperative efforts—and its working relationships with other federal agencies—are in their early stages of development and implementation. Currently, other federal agencies are providing staff to work directly with DNDO. However, it is too soon to determine the overall effectiveness of these efforts. DHS also works with other agencies to make current detection efforts more efficient and effective. For example, in April 2005, DHS and DOE entered into a memorandum of understanding to, among other things, exchange information on radiation detection technologies to improve the effectiveness of their deployment; the agencies also agreed to share lessons learned from operational experiences, and data received from radiation detection equipment deployed at U.S. and foreign ports. Also in April 2005, DHS entered into an agreement with the Port Authority of New York and New Jersey to, among other things, integrate lessons learned from field experience into domestic radiation detection efforts. In the future, DNDO intends to develop an integrated worldwide system. The resulting "global architecture," as it is being called by DNDO officials, would be a multi-layered defense strategy that includes programs that attempt to secure nuclear materials and detect their movements overseas, such as DOE's

Second Line of Defense program; to develop intelligence information on nuclear materials' trans-shipments and possible movement to the United States; and to integrate these elements with domestic radiation detection efforts undertaken by governments—federal, state, local, and tribal—and the private sector.

We are recommending a series of actions designed to help DHS speed up the pace of portal monitor deployments, better account for schedule delays and cost uncertainties, make the most efficient use of program resources, and improve its ability to interdict illicit nuclear materials.

We provided a draft of this report to DHS for its review and comment. DHS stated that it agreed with, and will implement, our recommendations.

Background

Initial concerns about the threat posed by nuclear smuggling were focused on nuclear materials originating in the former Soviet Union. As a result, the first major initiatives concentrated on deploying radiation detection equipment at borders in countries of the former Soviet Union and in Central and Eastern Europe. In particular, in 1998, DOE established the Second Line of Defense program, which, through the end of fiscal year 2005, had installed equipment at 83 sites mostly in Russia.[5] In 2003, DOE implemented a second program, the Megaports Initiative,[6] to focus on the threat posed by nuclear smuggling overseas by installing radiation

[5]We originally reported on U.S. efforts to combat nuclear smuggling in 2002. See GAO, *Nuclear Nonproliferation: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning*, GAO-02-426 (Washington, D.C.: May 16, 2002). See also, GAO, *Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries*, GAO-06-311 (Washington, D.C.: Mar. 14, 2006).

[6]We recently reported on the Megaports Initiative. See GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports*, GAO-05-375 (Washington, D.C.: Mar. 31, 2005).

detection equipment at major seaports around the world.[7] In the United States, the U.S. Customs Service began providing its inspectors with portable radiation detection devices in 1998. After September 11, 2001, the agency expanded its efforts to include the deployment of portal monitors—large-scale radiation detectors that can be used to screen vehicles and cargo.[8] In March 2003, the U.S. Customs Service was transferred to DHS, and the border inspection functions of the Customs Service, including radiation detection, became the responsibility of CBP.[9]

Deploying radiation detection equipment at U.S. borders is part of DHS's strategy for addressing the threat of nuclear and radiological terrorism. DHS's strategy includes: (1) countering proliferation at the source by assisting foreign governments in their efforts to detect and interdict nuclear and radiological smuggling; (2) controlling the illegal export of technology and equipment from the United States that terrorists could use to develop a nuclear or radiological weapon; (3) detecting and interdicting potential smuggling attempts before they reach the United States; and (4) securing U.S. ports-of-entry through multiple technologies that include radiation detection and nonintrusive inspections to view images of cargo in sea containers.

CBP plans to deploy radiation portal monitors in five phases, or "categories of entry": (1) international mail and express courier facilities; (2) major northern border crossings; (3) major seaports; (4) southwestern border crossings; and (5) all other categories, including international airports, remaining northern border crossings and seaports, and all rail crossings. In this final phase, CBP also plans to replace the currently-fielded portal monitors with newer, more advanced technology. Generally, CBP

[7]U.S. radiation detection assistance programs at foreign seaports are coordinated with—and complementary to—DHS's Container Security Initiative (CSI). Under CSI, which began operating in January 2002, U.S. Customs officials stationed in foreign ports review the cargo manifests of containers bound directly for the United States and attempt to identify containers with potentially dangerous cargo, such as explosives or weapons of mass destruction. GAO recently reported on CSI. See GAO, Container Security: *A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*, GAO-05-557 (Washington, D.C.: Apr. 26, 2005).

[8]We initially reported on the U. S. Customs Service's efforts to deploy radiation detection equipment at U.S. ports-of-entry in 2002. See GAO, *Customs Service: Acquisition and Deployment of Radiation Detection Equipment*, GAO-03-235T (Washington, D.C.: Oct. 17, 2002).

[9]See Pub. L. No. 107-296 (2002) and DHS Reorganization Plan (Nov. 25, 2002).

prioritized these categories according to their perceived vulnerability to the threat of nuclear smuggling. CBP did not, however, conduct a formal threat assessment. International mail and express courier facilities present a potential vulnerability because mail and packages arrive with no advance notice or screening. Northern border crossings are also vulnerable, according to CBP, because of the possible presence of terrorist cells operating in Canada. The third category, major seaports, is considered vulnerable because sea cargo containers are suitable for smuggling and because of the large volume of such cargo. Seaports account for over 95 percent of the cargo entering the United States. Southwestern borders are vulnerable because of the high volume of traffic and because of the smuggling that already occurs there. Although airlines can quickly ship and deliver air cargo, CBP considers air cargo to be a slightly lesser risk because the industry is highly regulated.

In deploying radiation detection equipment at U.S. borders, CBP identified the types of nuclear materials that might be smuggled, and the equipment needed to detect its presence. The radiological materials of concern include assembled nuclear weapons; nuclear material that could be used in a nuclear weapon but that is not actually assembled into a weapon ("weapons-grade nuclear material"); radiological disbursal devices, commonly called "dirty bombs;" and other illicit radioactive material, such as contaminated steel or inappropriately marked or manifested material. Detecting actual cases of attempted nuclear smuggling is difficult because there are many sources of radiation that are legal and not harmful when used as intended. These materials can trigger alarms (known as "nuisance alarms") that are indistinguishable from those alarms that could sound in the event of a true case of nuclear smuggling. Nuisance alarms are caused by patients who have recently had radiological treatment; a wide range of cargo with naturally occurring radiation, such as fertilizer, ceramics, and food products; and legitimate shipments of radiological sources for use in medicine and industry. In addition, detecting highly-enriched uranium, in particular, is difficult because of its relatively low level of radioactivity. Furthermore, a potential terrorist would likely attempt to shield the material to reduce the amount of radiation reaching the detector and thereby decrease the probability of detection.

The process of deploying portal monitors begins with a site survey to identify the best location at an entry point for installing the equipment. While in some cases the choice may be obvious, operational considerations at many entry points require analysis to find a location where all or most of the cargo and vehicles can pass through the portal monitor without

interfering with the flow of commerce. After identifying the best option, CBP works with local government and private entities to get their support. At many U.S. entry points, the federal government does not own the property and therefore collaborates with these entities to deploy the equipment. It is CBP's policy to depend exclusively on such negotiations, rather than to use any kind of eminent domain or condemnation proceeding. The actual installation of the portal monitors involves a number of tasks such as pouring concrete, laying electrical groundwork, and hooking up the portal monitors to alarm systems that alert officers when radiation is detected. Finally, PNNL tests the equipment and trains CBP officers on its operation, including how to respond to alarms.

To coordinate the national effort to protect the United States from nuclear and radiological threats, in April 2005, the president directed the establishment of DNDO within DHS. The new office's mission covers a broad spectrum of responsibilities and activities, but is focused primarily on providing a single accountable organization to develop a layered defense system. This system is intended to integrate the federal government's nuclear detection, notification, and response systems. In addition, under the directive, DNDO is to acquire, develop, and support the deployment of detection equipment in the United States, as well as to coordinate the nation's nuclear detection research and development efforts. For fiscal year 2006, DNDO's total budget is approximately $318 million, which includes at least $81 million for research and development of advanced nuclear detection technologies and $125 million for portal monitor purchase and deployment.

The Homeland Security Act of 2002 gave DHS responsibility for managing the research, development, and testing of technologies to improve the U.S. capability to detect illicit nuclear material.[10] Prior to the creation of DNDO, DHS's Science and Technology (S&T) directorate had this responsibility. DNDO has assumed these responsibilities and works with S&T's Counter Measures Test Beds (CMTB) to test radiation detection equipment in New York and New Jersey. As of January 2006, DNDO has provided $605,000 to DOE national laboratories that support this effort. Additional funding for fiscal year 2006 from S&T and DNDO to support test and evaluation activities at the CMTB is yet to be determined. The Homeland Security Act also provided DHS the authority to use DOE national laboratories for

[10]Pub. L. No. 107-296 (2002).

research, development, and testing of new technologies to detect nuclear material.[11]

DHS Has Made Progress in Deploying Radiation Detection Equipment, but the Agency's Program Goals Are Unrealistic and the Cost Estimate Is Uncertain

As of December 2005, DHS had completed deployment of portal monitors at two categories of entry—a total of 61 ports-of-entry—and has begun work on two other categories; overall, however, progress has been slower than planned. According to DHS officials, the slow progress has resulted from a late disbursal of funds, and delays in negotiating deployment agreements with seaport operators. Further, we believe the expected cost of the program is uncertain because DHS's plans to purchase newer, more advanced equipment are not yet finalized; also we project that the program's final cost will be much higher than CBP currently anticipates.

The Program to Install Portal Monitors Has Fallen Behind Schedule

Between October 2000 and October 2005, DHS, mainly through its prime contractor PNNL, has spent about $286 million to deploy radiation detection equipment at U.S. ports-of-entry. As of December 2005, DHS had deployed 670 of 3,034 radiation portal monitors—about 22 percent of the portal monitors DHS plans to deploy.[12] The agency has completed portal monitor deployments at international mail and express courier facilities and the first phase of northern border sites—57 and 217 portal monitors, respectively. In addition, by December 2005, DHS had deployed 143 of 495 portal monitors at seaports and 244 of 360 at southern borders. In addition, three portal monitors had been installed at the Nevada Test Site to analyze their detection capabilities and four had been retrofitted at express mail facilities. As of February 2006, CBP estimated that with these deployments CBP has the ability to screen about 62 percent of all containerized shipments entering the United States, and roughly 77 percent of all private vehicles (POVs). Within these total percentages, CBP can screen 32 percent of all containerized seaborne shipments; 90 percent of commercial trucks and 80 percent of private vehicles entering from Canada; and

[11]Pub. L. No. 107-296, § 309.

[12]CBP's most recent *Project Execution Plan* (December 2004) calls for deploying a total of 2,397 portal monitors. However, by December 2005, the scope of the deployments had grown to 3,034.

approximately 88 percent of all commercial trucks and 74 percent of all private vehicles entering from Mexico.

CBP does not maintain a firm schedule for deploying handheld radiation detectors, such as pagers and radiation isotope identification devices. This is equipment used mainly to help pinpoint and identify sources of radiation found during inspections. Instead, according to CBP officials, the agency acquires and deploys such equipment each fiscal year as needed. The handheld radiation detectors are procured to coincide with portal monitor deployments to ensure mission support. Since fiscal year 2001, CBP has spent about $24.5 million on pagers, and about $6.6 million on radiation isotope identification devices. At present, CBP can field roughly 12,450 pagers—enough to ensure that all officers conducting primary or secondary inspections at a given time have one. The agency intends to deploy about 6,500 additional pagers. Similarly, CBP's 549 radiation isotope identification devices are deployed at domestic ports-of-entry. CBP intends to acquire another 900 to ensure that all needs are met.

Overall, CBP and PNNL have experienced difficulty meeting the portal monitor deployment schedule. None of the planned portal monitor deployments has progressed according to schedule, and monthly deployments would have to increase by almost 230 percent to meet a September 2009 program completion date. For example, in November 2005, deployments at land crossings were about 20 months and $1.9 million behind schedule, while deployments at the first 22 seaports were about 2 years and $24 million behind schedule.[13] Despite these delays, PNNL reported in November 2005 that the overall project schedule should not extend beyond its current completion date of September 2009. However, our analysis indicates that CBP's deployment schedule is too optimistic.

[13]CBP and PNNL use an earned value management system (EVM) to report the domestic portal monitor deployment program's status against its baseline—scope, schedule, and budget. Essentially, an EVM approach compares the value of the work accomplished during a given period with the value of the work scheduled to be accomplished during that period. Differences from the schedule are measured in both cost and schedule "variances." For example, program activities (such as deploying portal monitors at a specific site) that are completed ahead of schedule would be reported as positive variances, while activities that are completed behind schedule would be reported as negative variances. Similarly, the EVM system tracks whether completed activities are costing more or less than expected. A negative cost variance would indicate that activities are costing more than expected, while a positive cost variance would mean activities are costing less than expected. We report schedule differences in both calendar and EVM terms. Appendix II provides more details on the EVM methodology and our analysis.

In fact, for CBP and PNNL to meet the current deployment schedule, they would have to install about 52 portal monitors per month from November 2005 to September 2009. In our view, this is unlikely because it requires a rate of deployment that far exceeds recent experience. For example, during calendar year 2005, PNNL deployed portal monitors at the rate of about 22 per month, and deployments have fallen further and further behind schedule. Between February and December 2005, for example, PNNL did not meet any of its scheduled monthly deployments, never deploying more than 38 portal monitors during any single month. If CBP continues to deploy portal monitors at its 2005 pace, the last monitor would not be deployed until about December 2014. Table 1 details the status of portal monitor deployments, as of December 2005.

Table 1: Status of Portal Monitor Deployments as of December 2005

Portal monitor deployment phase	Total portals planned	Status
International mail and express consignment facilities[a] (23 facilities)	57	Completed April 2004 4 months late
Land border and rail ports-of-entry (205 crossings)	967	20 months late
Seaports (106 terminals) and international airports	1,205	24 months late
Retrofits[b]	82[c]	Projected September 2009 completion
Other sites[d]	3	
Excess equipment[e]	721	
Total	**3,035**[f]	

Sources: PNNL and CBP.

[a]Excludes FedEx and UPS, both of whom screen packages overseas as agreed in a memorandum of understanding with CBP.

[b]"Retrofitting" refers to replacing currently-fielded portal monitors with advanced-technology portal monitors.

[c]PNNL plans a "net" increase of 82 portal monitors as a result of retrofits.

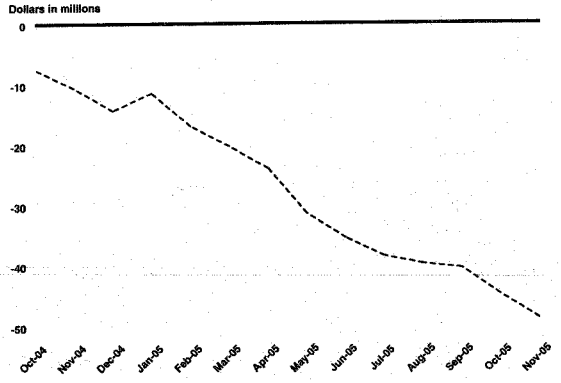
[d]"Other sites" refers to portal monitors installed at the Nevada Test Site for testing purposes.

[e]"Excess equipment" refers to the older portal monitors being replaced through the retrofit process.

[f]The total number of portal monitors planned for deployment is based on December 2005 estimates from CBP and PNNL. It represents a recent estimate of CBP's requirements, and according to CBP, it will be used to update the agency's current deployment plan, which calls for deploying 2,397 portal monitors by September 2009.

Further, we analyzed CBP's earned value management data as of November 2005 and determined that, although CBP planned for the deployment program to be 20.5 percent complete by that date, the program is only about 16 percent complete. In addition, our analysis indicates that since the program's inception, work valued at $48.6 million has fallen behind schedule. Moreover, the trend over the past 14 months shows CBP and PNNL falling further behind schedule, as seen in figure 1.

Figure 1: Monthly Cumulative Values of Work Planned but Not Finished As Planned



Source: GAO analysis based on the PNNL November 2005 Monthly Progress Report.

Note: The "zeropoint" on this figure denotes work that was completed at its planned cost. A positive number means that all the work completed to that point costs *less* than planned, while a negative number means that all the work completed to that point costs *more* than planned.

There have been at least three major sources of delay that have affected the portal monitor deployment program: funding issues, negotiations with seaport terminal operators, and problems in screening rail cars—particularly in a seaport environment.

Funding Issues

According to CBP and PNNL officials, recurrent difficulties with the project's funding are the most important explanations of the schedule delays. Specifically, according to DHS and PNNL officials, CBP has been chronically late in providing appropriated funds to PNNL, thereby hindering its ability to meet program deployment goals. For example, PNNL did not receive its fiscal year 2005 funding until September 2005. According to PNNL officials, because of this delay, some contracting activities in all deployment phases had to be delayed or halted, but the adverse effects on seaports were especially severe. For example, PNNL reported in August 2005 that site preparation work at 13 seaports had to cease because the Laboratory had not yet received its fiscal year 2005 funding allocation. According to senior CBP officials, their agency's inability to provide a timely spending plan to the Congress for the portal monitor deployment program is the main reason for these funding delays. According to the House Appropriations Committee report on the CBP portion of DHS's fiscal year 2005 budget, CBP should provide the Congress an acquisition and deployment plan for the portal monitor program prior to funding PNNL.[14] However, these plans typically take many months for CBP to finalize—in part because CBP requires that the plans undergo several levels of review—but also because these plans are reviewed by DHS and OMB before being submitted to the Congress. In fiscal year 2005, this process was further delayed by the creation of DNDO, uncertainty regarding DNDO's responsibilities, and negotiations regarding the expenditure of the fiscal year 2005 appropriations.

CBP has tried to address this problem by reprogramming funds when money from other programs is available. In some cases, the amount of reprogrammed funds has been fairly large. For example, about 15 percent of fiscal year 2005's funding included money reprogrammed from other CBP sources, or almost $14 million. In fiscal year 2004, about $16 million was reprogrammed—or about a third of the fiscal year's total. And in fiscal year 2003, the total of reprogrammed money was about $18 million—about 20 percent.

Delays in Gaining Agreements Have Slowed Seaport Deployments

Negotiations with seaport operators have been slow and have also delayed the portal monitor deployment program. According to CBP and PNNL officials, one of the primary reasons behind the seaport phase's substantial delay in deployments is the difficulty in obtaining contractual agreements

[14] H.R. Rep. No. 108-541, at 25-26 (2004).

with port and terminal operators at seaports. DHS has not attempted to impose agreements on seaport operators because, according to officials, cooperative arrangements with the port operators are more efficient and, in the long term, probably more timely. According to CBP and PNNL officials, many operators believe screening for radiation will adversely affect the flow of commerce through their ports. In addition, deploying portal monitors in major seaports presents several unique challenges. For example, seaports are much larger than land border crossings, consist of multiple terminals, and may have multiple exits. Because of these multiple exits, seaports require a greater number of portal monitors, which may entail more negotiations with port and terminal operators. In addition, port operators at times have insisted on late-stage design changes, requested various studies prior to proceeding with final designs, insisted on inefficient construction schedules, and delayed their final review and approval of project designs. According to CBP and PNNL, these efforts often reflect the port and terminal operators' uneasiness with portal monitor deployments, and their resolve to ensure that the outcome of the deployment process maintains their businesses' competitiveness. For example, port officials at one seaport requested several changes late in the process, including performing an unscheduled survey for laying cable, revising portal monitor locations at two gates, and adding a CBP control booth at a third terminal. According to CBP and PNNL officials, the agency prefers to accommodate these types of changes, even late in the process and even if they slow deployment, because in the long term they believe it is more efficient and effective.

Screening Rail Cars in Seaports Presents Unique Problems

The difficulty of devising an effective and efficient way to conduct secondary inspections of rail traffic departing seaports without disrupting commerce has created operational issues that could further delay deployments. Four of the five seaports we visited employ rail cars to ship significant amounts of cargo. In one seaport, the port director estimated that about 80-85 percent of the cargo shipped through his port departs via rail. For the other three seaports, the percentages for rail traffic were 5 percent, 13 percent, and 40 percent respectively. According to port officials, these seaports would like to accommodate CBP's efforts to install radiation detection equipment designed to screen rail traffic, but they are concerned that the logistics of conducting secondary inspections on trains as they prepare to depart the seaport could back up rail traffic within the port and disrupt rail schedules throughout the region—potentially costing the port tens of thousands of dollars in lost revenue. For example, one senior port authority official told us that his port lacked ample space to park trains for secondary inspections, or to maneuver trains to decouple

the rail car(s) that may have caused a primary inspection alarm. As a result, trains that cause a primary alarm would have to wait, in place, for CBP to conduct a secondary inspection, blocking any other trains from leaving the port. According to this port official, any delay whatsoever with a train leaving the port could cause rail problems down the line because track switches are geared to train schedules. To avoid these kinds of problems, CBP has delayed deploying portal monitors in this seaport until technical and operational issues can be overcome. As of December 2005, no portal monitors had been deployed at this seaport, although according to PNNL's schedule, 5 of its 11 terminals—a total of 19 portal monitors—should have been deployed by October 2005. According to the port director at another seaport we visited, a port that actually has a rail portal monitor installed, similar operational issues exist. However, in addition to backing up rail traffic within the port, trains awaiting secondary inspections at this port could block the entrance/exit to a nearby military base. The director of the state's port authority told us that his solution has been to simply turn off the portal monitor. According to CBP officials, this was entirely a state decision, since this portal monitor is the state's responsibility and not part of CBP's deployment. However, these officials also noted that they agreed with the states and noted that they would not attempt to impose a solution or deadline on either port. CBP officials noted that most seaport operators seem willing to accommodate portal monitors, but until a better portal monitor technology evolves that can help ensure a smooth flow of rail traffic out of the port, negotiations with seaport operators will continue to be slow.

According to CBP and port officials, they have considered several potential solutions. For example, there is widespread agreement that screening sea cargo containers *before* they are placed on rail cars offers the best solution, but this option is operationally difficult in many seaports. Mobile portal monitors, when commercially available, may also offer a partial solution. In addition, CBP is optimistic that advanced portal monitors, when they become commercially available, may help solve some of the problems in the rail environment by limiting the number of nuisance alarms. However, according to the CBP and port officials we contacted, screening rail traffic continues to pose a vexing operational problem for seaports.

The concerns that seaport operators and CBP expressed regarding screening rail commerce in seaports may increase and intensify in the future because rail traffic, in general, is expected to increase substantially by 2020. DOT has forecast that by 2020, rail will transport roughly 699 million tons of international freight—up from 358 million tons carried in

1998. Officials at 3 of the 5 seaports we visited expect rail traffic through their facilities to increase dramatically during the next 10 to 15 years. As the volume of trade increases, so too will the economic stakes for the port and terminal operators, while the regulatory burden for CBP is likely to increase as well. Delays—for any reason, including radiation detection—are likely to become more costly, and CBP will likely have ever-increasing numbers of rail cars to screen.

In addition, although CBP is not scheduled to begin deploying portal monitors to screen rail shipments at land border crossings until 2007, the agency will likely experience operational challenges at land border crossing similar to those it is now experiencing at seaports. For example, at both land border crossings and seaports, if a rail car alarms as it passes through a portal monitor, that car will possibly have to be separated from the remaining train—sometimes a mile in length—to undergo a secondary inspection. Furthermore, because trains transport numerous types of cargo containing large quantities of naturally occurring radioactive material, CBP faces the challenge of maintaining a nuisance alarm rate that does not adversely affect commerce. CBP and PNNL are currently conducting testing of a prototype rail portal monitor to determine the potential impact of naturally occurring radioactive material on rail operations at land border crossings.

Other Factors Have Delayed Portal Monitor Deployments

Unforeseen design and construction problems have also played a role in delaying portal monitor deployments. For example, deployments at six southern border sites have been delayed to coincide with the sites' expansion activities. According to CBP officials, there are two approaches to accommodating a port-of-entry's alterations, both of which may delay portal monitor deployments. First, CBP and PNNL may decide to delay the start of portal monitor projects until the port-of-entry completes its alterations, to make certain that portal monitor placements are properly located. Second, port-of-entry expansion activities may alter existing traffic flows and require that PNNL redesign its portal monitor deployments. The portal monitor deployments at three southern border ports-of-entry has taken much longer than planned because of the port's expansion activities. According to PNNL, there is now considerable schedule uncertainty associated with these deployments, which may ultimately impact the completion of the southern land border deployments.

Portal monitor deployments have also been hampered by poor weather. For example, cold weather at several northern sites caused some unexpected work stoppages and equipment failures that resulted in

construction delays of 2 to 3 months. Finally, one southern border site has been delayed because of major flooding problems. The flooding issue must be resolved before the deployment can be completed.

DHS's Portal Monitor Deployment Program Cost Estimate Is Uncertain and Overly Optimistic

DHS's current estimate to complete the program is $1.3 billion, but this estimate is highly uncertain and overly optimistic. First, DHS's cost estimate is based on a plan to deploy advanced-technology portal monitors that have so far shown mixed results for detecting radiation compared to currently-fielded portal monitors. Since the efficacy of the advanced portal monitors has not yet been proven conclusively, there is at least some uncertainty over whether—and, if so, how many—of the new portal monitors may be deployed. In addition, the final cost of the new portal monitors has not been established. Second, our analysis of CBP's earned value data also suggests that the program will likely cost much more than planned.

The current deployment plan calls for installing advanced portal monitors at all cargo primary and secondary inspection locations, at all secondary inspection locations for private vehicles, and also retrofitting many sites with the advanced equipment, when it becomes available. However, according to senior officials at DNDO, the advanced technology must meet all of DNDO's performance criteria, and must be proven superior to the portal monitors already in use, before DNDO will procure it for use in the United States. Recent tests of the new portal monitors indicate that DNDO's criteria have not yet been met. For example, S&T sponsored research in 2004 that compared the detection capabilities of currently-fielded portal monitors with the advanced portal monitors. The results of that research suggested that, in some scenarios, the detection abilities of the two portal monitor types were nearly equivalent. In other scenarios, the new equipment's detection capability was significantly better. S&T concluded that more work remains to be done in optimizing and comparing portal monitors so as to understand how they can be used to the greatest effect at U.S. ports-of-entry. In 2005, DNDO sponsored additional research designed to compare the two types of portal monitor, and determined that the advanced portal monitors' detection capabilities were somewhat better than those of the currently-fielded equipment. In addition, in October 2005, DNDO completed the first comprehensive tests for these advanced portal monitors at the Nevada Test Site. This advanced technology combines the ability to detect radiation and identify its source. According to an official who helped supervise these tests, the new portal monitors' performance did not meet all of DNDO's expectations with regard to providing

significant detection improvements over currently-fielded equipment in all scenarios. CBP and DNDO officials also expressed concerns regarding the advanced portal monitors' detection capabilities in light of the Nevada test results. In particular, senior CBP officials questioned whether the advanced portal monitors would be worth their considerable extra costs, and emphasized finding the right mix of current and advanced-technology equipment based on the needs at individual ports-of-entry. According to DNDO officials, the potential improvement over currently fielded portal monitors in capability to identify radioactive sources, and hence to detect actual threats as opposed to simply detecting radiation, has not yet been quantified. However, these officials believe that the results to date have been promising, and DNDO intends to continue supporting the advanced portal monitor's development and believe the new technology may be ready for deployment early in calendar year 2007.

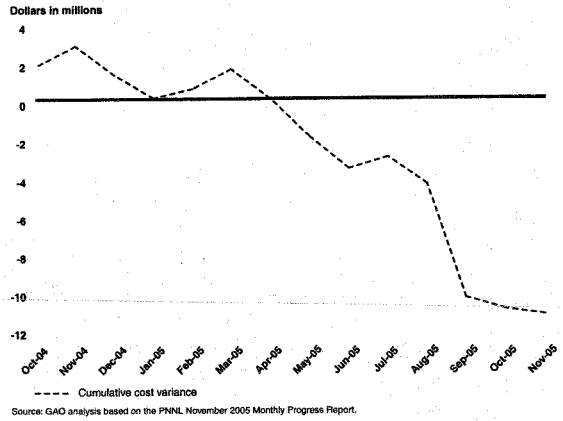
There is also considerable uncertainty regarding the eventual cost of the advanced portal monitors—if they become commercially available, and if DNDO opts to use them. Experts we contacted estimated that the new portal monitors could cost between $330,000 and $460,000 each. These estimates are highly uncertain because advanced portal monitors are not yet commercially available. As a point of reference, the portal monitors currently in use typically cost between $49,000 and $60,000. These costs include only the purchase price of the equipment, not its installation. According to CBP and PNNL officials, installation costs vary, but average about $200,000 per portal monitor. Even if future test results indicate that the new technology exhibits much better detection and identification capabilities, it would not be clear that the dramatically higher cost for this new equipment would be worth the considerable investment, without the agency having first rigorously compared the portal monitors' capabilities taking their costs into account. Currently, DNDO and CBP are working together to determine the most appropriate technologies and concepts of operation for each port-of-entry site. The two agencies are also trying to determine the highest priority sites for advanced-technology portal monitors based on the extent to which the new portal monitors show improved performance.

In November 2005, PNNL reported that the portal monitor deployment program could experience an overall cost overrun of $36 million. In contrast, our analysis of CBP's earned value data indicates that the agency should expect a cost overrun of between $88 million and $596 million. We based our cost overrun projections on the rates at which CBP and PNNL deployed portal monitors, through November 2005. The more efficient the

agency and its contractor are in deploying portal monitors, the smaller the cost overruns; conversely, when efficiency declines, cost overruns increase.[15]

In fact, as shown in figure 2, recent cumulative program cost trends have been negative, indicating that CBP's cost overruns are deepening over time.

Figure 2: Monthly Cumulative Cost Overruns



Source: GAO analysis based on the PNNL November 2005 Monthly Progress Report.

Note: The "zero point" on this figure denotes work that was completed at its planned cost. A positive number means that all the work completed to that point costs *less* than planned, while a negative number means that all the work completed to that point costs *more* than planned.

[15]We also assessed PNNL's cost and schedule performance using earned value analysis techniques based on data captured in PNNL's contract performance reports. We also developed a forecast of future cost growth. We based the lower end of our forecast range on the costs spent to date added to the forecast cost of work remaining. The remaining work was forecast using an average of the current cost performance index efficiency factor. For the upper end of our cost range, we relied on the actual costs spent to date added to the forecast of remaining work with an average monthly cost and schedule performance index.

PNNL noted that its management reserve of $62 million should cover the anticipated overrun. However, we do not agree.[16] First, we believe the cumulative cost overrun will far exceed PNNL's estimate of $36 million. We believe an overrun of about $342 million, the midpoint of our projected overrun range, is more likely. Since 1977, we have analyzed over 700 acquisition projects on which EVM techniques have been applied. These analyses consistently show that once a program is 15 percent complete (as is the case with this program), cost performance almost never improves and, in most cases, declines. PNNL's recent cost trend follows this pattern. Second, based on these 700-plus studies, our estimate takes a more realistic view that the portal monitor deployment program's cost performance most likely will continue to decline; hence the management reserve will be consumed over time as the program incurs unexpected expenses. Finally, to meet the deployment program's planned costs, PNNL would have to greatly improve its work efficiency. However, our analysis of prior EVM-based projects indicates that productivity rates nearly always decline over the course of a project. We determined that PNNL's efficiency rate for the most recent 8 months has averaged about 86 percent—PNNL has been delivering about $.86 worth of work for every dollar spent. In order to complete the remaining work with available funding, PNNL's efficiency rate would have to climb to around 98 percent, a rate of improvement unprecedented in the 700-plus studies we have analyzed.

CBP Does Not Know If PNNL's Cost and Schedule Data Are Reliable

Federal agencies are required by OMB to track the progress of major systems acquisitions using a validated EVM system and to conduct an integrated baseline review.[17] We found that PNNL has an EVM system but has not certified it to show that it complies with guidance developed by the American National Standards Institute/Electronic Industries Alliance.[18] This guidance identifies 32 criteria that reliable EVM systems should meet. In addition, we found that PNNL has not conducted an integrated baseline review—a necessary step to ensure that the EVM baseline for the portal

[16]Management reserves are part of the total program budget intended to be used to fund work anticipated but not currently defined. Most programs usually wait until work is almost completed before making a judgment that management reserve can be applied to cover cost variances.

[17]See OMB Circular No. A-11, Part 7, "Planning, Budgeting, Acquisition, and Management of Capital Assets," June 2005.

[18]American National Standards Institute (ANSI) / Electronic Industries Alliance (EIA) EVM System Standard (ANSI/EIA-748-98), Chapter 2 (May 19, 1998).

monitor program represents all work to be completed, and adequate resources are available.

However, although the EVM data have not been independently validated, we examined the EVM data and found that they did not show any anomalies and were very detailed. Therefore, we used them to analyze the portal monitor program status and to make independent projections of the program's final costs at completion.

CBP Officers Have Made Progress in Using Radiation Detection Equipment Correctly and Adhering to Inspection Guidelines, but There Are Potential Issues with Agency Procedures

CBP officers we observed conducting primary and secondary inspections appeared to use radiation detection equipment correctly and to follow the agency's inspection procedures. In fact, in some cases, CBP officers exceeded standard inspection procedure requirements by opening and entering containers to better identify radiation sources. In contrast, in 2003, when we issued our last report on domestic radiation detection, CBP officers sometimes deviated from standard inspection procedures and, at times, used detection equipment incorrectly. However, the agency's inspection procedures could be strengthened.

CBP Officers Appeared to Use Equipment Correctly and Follow Procedures

During this review, at the 10 ports-of-entry that we visited, the CBP officers we observed conducting primary and secondary inspections appeared to follow inspection procedures and to use radiation detection equipment correctly. The officers' current proficiency in these areas follows increases in training and in CBP's experience using the detection equipment. In contrast, in 2003 we reported that CBP officers sometimes used radiation detection equipment in ways that reduced its effectiveness.

CBP has increased the number of its officers trained to use radiation detection equipment; in fact, the agency now requires that officers receive training before they operate radiation detection equipment. As of February 2006, CBP had trained 6,410 officers to use radiation isotope identification devices, 8,461 to use portal monitors, and 22,180 to use pagers. Many CBP officers received training on more than one piece of equipment and about 900 have since left the agency. Generally, today CBP officers receive radiation detection training from 4 sources: the CBP Academy in Glynco, Georgia; the Border Patrol Academy in Artesia, New Mexico; a DOE-

sponsored 3-day training course for interdicting weapons of mass destruction, in Washington state; and on-the-job training at ports-of-entry. Training at the Academies in Georgia and New Mexico includes formal classroom instruction, as well as hands-on exercises on how to use portal monitors, isotope identifiers, and pagers. This training includes simulated scenarios in which officers use radiation detection equipment to conduct searches for nuclear and radiological materials. On-the-job instruction continues at field locations as senior CBP officers, as well as PNNL and other DHS contractor staff, work closely with inexperienced officers to provide them with practical training on how the radiation detection equipment works and how to respond to alarms. According to senior CBP officials, all of the instructors that offer training on using radiation detection equipment are certified in its use. Trainees must demonstrate proficiency in the use of each system prior to assuming full responsibility for radiation detection inspections. About 1,600 CBP officers have participated in DOE's 3-day training course designed to acquaint CBP officers with detection equipment. CBP is currently developing refresher training courses on the use of radiation detection equipment. To further enhance officers' ability to effectively respond to real or potential threats, several of the field locations that we visited conduct "table-top exercises" that simulate scenarios in which the equipment detects an illicit radiological source.

According to several of the CBP field supervisors we contacted, many officers have gained proficiency in following procedures and using radiation detection equipment through substantial field experience responding to alarms. The number of alarms officers typically handle varies according to the size of the site, its location, and type. For example, an isolated land border site would probably experience fewer alarms than a major seaport because of the differences in the volume of traffic. However, it was common for several of the locations we visited to experience 15 to 60 alarms per day. One seaport we visited had 9 terminals, usually with 2 primary and 1 secondary portal monitors. According to CBP officials, each terminal recorded about 8 to 12 alarms per day. The director of port security for a major eastern seaport we visited estimated that her facility records roughly 150 portal monitor alarms each day. Virtually all have been nuisance alarms, but CBP officials still believe they gained valuable experience in using the equipment and following procedures.

All of the primary and secondary inspections we witnessed were nuisance alarms. In all of these cases except one, officers followed CBP's guidance—as well as local variations meant to address issues unique to the area—and

correctly used detection equipment. The lone exception occurred at a site whose primary inspection station was staffed by a state port police officer. After the station's portal monitor registered an alarm for a truck departing the site, the police officer did not follow CBP's procedures.[19] For example, he did not collect any documentation from the driver. At all other sites we visited, when a primary portal monitor sounded, CBP officers gathered the cargo's manifest, the vehicle registration, and the driver's license prior to sending the vehicle through secondary inspection. Officers use these documents to check the driver and vehicle cargo. The port police officer told us that he recognized the driver in this case, and so the officer did not believe it was necessary to collect such information. A CBP officer performed the secondary inspection in line with agency guidance. In fact, after using a radiation isotope identification device to conduct an external inspection and determine the source of the alarm—potassium hydroxide—the officer required that the driver open the back of the truck so she could make a visual check of the cargo. From the time of the initial alarm, until the truck departed the site boundary, about 35 minutes elapsed. According to port and CBP officials, this particular alarm, its resolution, and the amount of time it took to resolve are typical of the site. We also discussed the site's radiation detection efforts with the truck driver, in particular the delay associated with this alarm. He noted that he considers the delays experienced at this site to be relatively minor, and that the delays have not had any adverse effects on his business.

We also visited a seaport that experienced a legitimate alarm in which CBP officers used the detection equipment correctly and responded according to procedures. Uranium hexafluoride, a potentially hazardous chemical containing low levels of radioactivity, caused this alarm. A primary portal monitor at the seaport sounded as a truck carrying one container attempted to exit a terminal. Following standard operating procedures, the truck was diverted to a secondary inspection station, where a secondary portal monitor also alarmed. A CBP officer then scanned the container and cab of the truck with an isotope identifier, which indicated that the radiation source was located in the cab within several metal pails. The isotope identifier identified two radiation sources, one of which was uranium-235—potentially a weapons-usable material. The other source was uranium-238. Again following procedures, CBP officers isolated the

[19]Since the officer is an employee of the state, he was not required to follow CBP procedures. According to the port police supervisor present at the scene, the officer acted within the scope of port police guidance.

sources of radiation and provided LSS scientists with information collected by the isotope identifier. Officers also reviewed the driver's delivery papers; used various CBP databases to check the driver, importer, and consignee's history of transporting goods; and contacted the driver's dispatcher and the U.S. consignee to gather information on and assess the legitimacy of the shipment. The consignee explained that the pails contained trace amounts of uranium hexafluoride that had been sent to the company's laboratory for testing. Following additional investigation, which included an X-ray of the pails and a review of DOT requirements regarding radiation-warning placard requirements, CBP determined that the event was not a security threat and released the driver and conveyance. Senior officials at this seaport told us that CBP's radiation detection guidance served as an effective and successful guide to resolving this alarm.

Potential Issues in CBP's Inspection Procedures Could Be Mitigated to Improve Detection Capabilities

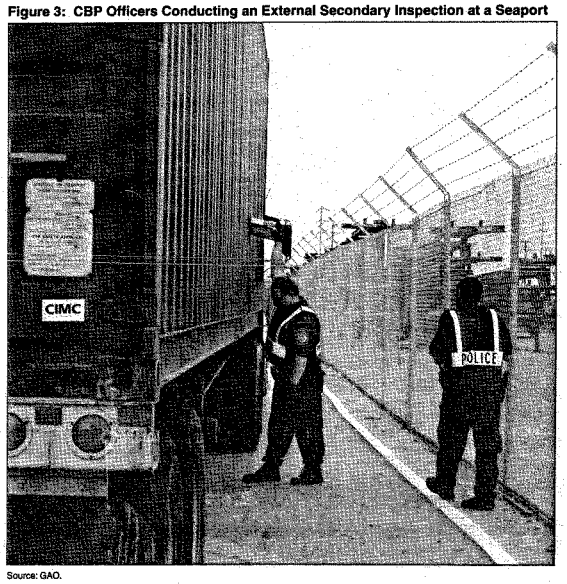
We identified two potential issues in CBP's national inspection procedures that could increase the nation's vulnerability to nuclear smuggling. The first potential issue involves NRC documentation. Generally, NRC requires that importers obtain an NRC license for their legitimate shipments of radiological materials into the United States.[20] However, NRC regulations do not require that the license accompany the shipment, although in some cases importers choose to voluntarily include the license. According to CBP officials, CBP lacks access to NRC license data that could be used to verify that importers actually acquired the necessary licenses or to authenticate a license at the border. At present, CBP officers employ a variety of investigative techniques to try to determine if individuals or organizations are authorized to transport a radiological shipment. For example, CBP officers review their entry paperwork, such as shipping papers. Officers also often interview drivers about the details of the delivery and observe their behavior for any suspicious or unusual signs. At one land border crossing we visited, officers told us that frequent and legitimate shippers of radiological material provide advance notice that a radiological shipment will be transported. This can lead to law enforcement personnel being called in to escort the shipment through the port-of-entry.

The second potential issue pertains to CBP's secondary inspection guidelines. Generally, CBP's guidelines require that CBP officers locate,

[20]See 10 C.F.R. § 110.5.

isolate, and identify the radiation source(s) identified during primary inspections. Customarily, officers use a radiation isotope identification device to perform an external examination of cargo containers in these situations. (See fig. 3.) However, the effectiveness of a radiation isotope identification device is diminished as its distance from the radioactive source increases, and by the thickness of the metal container housing the radioactive source. As a result, secondary inspections that rely solely on external examinations may not always be able to locate, isolate, and identify an illicit shipment of nuclear material.

Figure 3: CBP Officers Conducting an External Secondary Inspection at a Seaport



Source: GAO.

The local procedures at some ports-of-entry we visited go beyond the requirements established by CBP's guidelines by having CBP officers open and, if necessary, enter containers when conducting secondary inspections. (See fig. 4.) For example, at one high-volume seaport we visited, the local inspection procedures require officers to open and, if necessary, enter a container to locate and identify a radiological source if an external examination with an isotope identifier is unable to do so. Under such circumstances, the port's procedures require the officer to open the container doors, locate the source, and obtain another reading as close to the source as possible. By entering the container, an officer may be able to reduce the isotope identifier's distance from the radioactive source, and thus obtain a more accurate reading. If the isotope identifier is unable to detect and identify the source after two readings within the container, officers must contact LSS for further guidance. Officers at this seaport have opened containers in the past when the isotope identifier had been unable to detect naturally occurring radioactive material, such as granite or ceramic tile, which is low in radioactive emissions. CBP supervisors at this seaport said that this occurs infrequently and that it adds a very minimal amount of time to the inspection process. In addition, at a land border crossing we visited, the local standard operating procedures instruct CBP officers to conduct a physical examination on vehicles that alarm for the presence of radiation. Officials at this particular port-of-entry said that they have entered vehicles with an isotope identifier when the device has been unable to detect or identify the radioactive source from vehicles' exterior. During a physical examination, officers are supposed to open the vehicle and look for high-density materials, such as lead or steel, which can be used to shield gamma radiation and solid objects with large quantities of liquid that could be used to shield neutron radiation. Because the majority of alarms at this land border crossing are caused by medical isotopes in people, CBP officers physically inspect vehicles on an infrequent basis.

Figure 4: A CBP Officer Entering a Cargo Container During a Secondary Inspection at a Seaport

Source: GAO.

Finally, we also visited a land border crossing where CBP officers routinely open and enter commercial trucks to conduct secondary inspections, even though the site's local procedures do not require this additional examination. Officials at this crossing said that they open up containers to verify that the container's manifest and reading from the isotope identifier are consistent with the container's load. If they are not consistent, CBP officers are supposed to contact LSS for further guidance. During our visit, we observed a truck that alarmed at primary and secondary portal monitors. CBP officers then required the driver to park at a loading dock, where officers first used an isotope identifier to screen the truck from the outside; the reading from the isotope identifier was inconclusive, however. Officers then opened and entered the container with an isotope identifier, conducted a second reading of the radioactive source, and determined that the material inside the container was a non-threatening radioactive source that matched the manifest. A CBP supervisor released the truck. This inspection, from the time of the original alarm to the truck's release took about 25 minutes—slightly greater than the 20-minute average for this site. According to CBP supervisors, officers at this port-of-entry follow this practice routinely, even during the site's peak hours. This approach enables the officers to get closer to the source and obtain a more accurate reading. Furthermore, since this practice enables officers to conduct a more thorough examination of the containers' contents, it may increase the likelihood that CBP officers will find any illicit radioactive material. According to senior CBP officials at this port-of-entry, despite being implemented at one of the busiest commercial ports-of-entry in the nation, this additional procedure has had little negative impact on the flow of commerce and has not increased the cost of CBP inspections.

DHS Is Working to Improve the Capabilities of Currently-fielded and New Radiation Detection Equipment, but Much Work Remains to Achieve Better Equipment Performance

DHS has managed research, development, and testing activities that attempt to address the inherent limitations of currently-fielded radiation detection equipment and to produce new, advanced technologies with even greater detection capabilities. DHS is enhancing its ability to test detection equipment by building a new test facility at DOE's Nevada Test Site. In addition, DHS tests radiation detection equipment under real-life conditions at S&T's CMTB in New York and New Jersey. However, much work remains for the agency to achieve consistently better detection capabilities, as the efforts undertaken so far have achieved only mixed results.

Currently-fielded Radiation Detection Equipment Has Inherent Limitations

Currently-fielded radiation portal monitors have two main limitations. First, they are limited by the physical properties of the radiation they are designed to detect, specifically with regard to the range of detection (some radioactive material emits more radiation than others). Further, this limitation can be exacerbated because sufficient amounts of high-density materials, such as lead or steel, can shield radiation emissions to prevent their detection. Second, currently-fielded portal monitors cannot distinguish between different types of radioactive materials, i.e., they cannot differentiate naturally occurring radioactive material from radiological threat materials. CBP officers are required to conduct secondary inspections on all portal monitor alarms, including nuisance alarms. According to the CBP field supervisors with whom we spoke, nuisance alarms comprise almost all of the radiation alerts at their ports-of-entry. Port operators noted a concern that nuisance alarms might become so numerous that commerce could be impeded, but thus far these alarms have not greatly slowed the flow of commerce through their ports-of-entry.

CBP's currently-fielded radiation isotope identification devices also have inherent limitations. For example, during some secondary inspections, radiation isotope identification devices are unable to identify radiological material. In these cases, CBP standard procedures require that officers consult LSS to conclusively identify the source. According to CBP officers at two of the ports we visited, this usually lengthens secondary inspections by 20 to 30 minutes, although in some cases an hour or more was needed to resolve the alarm. Furthermore, a 2003 Los Alamos National Laboratory

evaluation of seven isotope identifiers, including the one deployed by CBP, concluded that all devices had difficulty recognizing radioactive material and correctly identifying the material they did recognize. The Los Alamos finding is consistent with our field observations, as CBP officers at several of the ports-of-entry we visited reported similar trouble with their radiation isotope identification devices.

Laboratory testing of currently-fielded radiation detection equipment has further demonstrated their limitations in effectively detecting and identifying nuclear material. For example, in February 2005, DHS sponsored testing of commercially available portal monitors, isotope identifiers, and pagers against criteria set out in American National Standards Institute (ANSI) standards. The ANSI standards provide performance specifications and test methods for testing radiation detection equipment, including portal monitors and handheld devices. The actual testing was performed by four DOE laboratories, with coordination, technical management, and data evaluation provided by the Department of Commerce's National Institute for Standards and Technology (NIST). The laboratories tested a total of 14 portal monitors from 8 manufacturers against 29 performance requirements in the ANSI standards. Overall, none of the radiation detection equipment, including the portal monitors and handheld devices deployed by CBP, met all of the performance requirements in this first round of testing. However, according to S&T officials, many of the limitations noted in CBP's equipment were related to withstanding environmental conditions—not radiation detection or isotope identification. However, in some tests, the portal monitors that CBP employs, along with many others, exhibited poor results. For example, in tests conducted to evaluate the portal monitors' response to neutron radiation, of which plutonium is a primary source, almost all monitors, including a portal monitor fielded by CBP, failed to meet the ANSI requirement. However, according to S&T officials, the test was conducted using the manufacturer's standard configuration, rather than the configuration CBP uses in its field operations. In another test, one that used CBP's typical field parameters rather than the manufacturer's, the portal monitor passed all the radiation detection performance requirements. S&T believes that the portals used by CBP would meet all the radiation performance requirements if set up with the parameters and configuration as used in the field. In addition, isotope identifiers displayed weaknesses. For example, the isotope identifier currently in use by CBP was not able to simultaneously identify two different isotopes, as required by the ANSI standards. When tested with barium-133 and plutonium-239, the isotope identifier was able to recognize the barium but failed to recognize the

plutonium—a weapons-grade nuclear material. As this was a first round of testing and modifications were made to both the standards and testing protocols after the procedures were completed, NIST plans to manage testing of the equipment again in early 2006. The results from both rounds of testing are intended to provide guidance for federal, state, and local officials in evaluating and purchasing radiation detection equipment, and to enable manufacturers to improve their equipment's performance.

DHS Has Sponsored Research and Development to Improve the Capabilities of Current Technology and to Develop New Technology but Much Work Remains

DHS has sponsored research efforts designed to improve the detection capabilities of the currently-fielded portal monitors and to provide them with the ability to distinguish radiological sources. For example, PNNL researched, developed, and tested a new software—known as "energy windowing"—to address the currently-fielded portal monitors' inability to distinguish between radiological materials. Energy-windowing is supposed to identify and screen out material, such as fertilizer or kitty litter, that cause nuisance alarms and thereby reduce the number of such alarms at cargo screening facilities, while also improving the portal monitor's sensitivity to identify nuclear material of concern. PNNL has activated energy-windowing on the 556 portal monitors it has deployed at land border crossings and seaports. At a few ports-of-entry that we visited, CBP officials said that the software has been effective in significantly reducing the number of nuisance alarms. However, tests of the software have shown that its effectiveness in reducing nuisance alarms largely depends on the types of radiation sources it has been programmed to detect and differentiate. In tests involving some common, unshielded radiation sources, such as cobalt-57 and barium-153, the new software has shown improved detection and discrimination capabilities. However, during scenarios that target other common, shielded threat sources—such as those that might be used in a shielded radiological dispersal device or nuclear weapon—the software has been less able to detect and discriminate. Experts have recommended further testing to fully explore the software's capabilities.

DHS is also sponsoring the development of three new technologies that are designed to address the main inherent limitations of currently-fielded portal monitors. CBP's deployment plan currently calls for the widespread installation of the first of these technologies, "advanced spectroscopic portal monitors." According to DNDO, the advanced spectroscopic technology uses different detection materials that are capable of both detecting the presence of radiation and identifying the isotope causing the alarm. It is hoped that the spectroscopic portal monitor can more quickly

identify the sources of alarms, thereby reducing the number of nuisance alarms. This increased operational effectiveness may allow the portal monitors to be set at a lower detection threshold, thus allowing for greater sensitivity to materials of concern. DHS commissioned PNNL to determine whether spectroscopic portal monitors provide improved performance capabilities over the currently-fielded monitors. In July 2004 and July 2005, PNNL conducted two small-scale preliminary studies to compare the two types of portal monitors in side-by-side tests using shielded and unshielded radioactive materials. In the first test, PNNL concluded that the relative performance of spectroscopic and currently-fielded portal monitors is highly dependent on variables such as the radioactive sources being targeted and the analytic methods being used. The results of these tests were mixed. In some situations, spectroscopic portal monitors outperformed the current technology; in other cases, they performed equally well. In the second test, PNNL concluded that the spectroscopic monitor's ability to detect the shielded threat sources was equal to, but no better than, those of the currently-fielded portal monitors. However, because spectroscopic portal monitors have the ability to identify isotopes, they produced fewer nuisance alarms than the current portal monitors. PNNL noted that because the studies were limited in scope, more testing is needed.

In October 2005, DNDO completed the first round of comprehensive testing of spectroscopic portal monitors at its testbed at the Nevada Test Site. DNDO tested 10 spectroscopic portal monitors against 3 currently-fielded monitors in 7,000 test runs involving the portal monitors' ability to detect a variety of radiological materials under many different cargo configurations. According to senior DNDO officials who supervised these tests, preliminary analysis of test data indicates that the spectroscopic portal monitors' performance demonstrated somewhat mixed results. Spectroscopic portal monitors outperformed currently-fielded equipment in detecting numerous small, medium-sized, and threat-like radioactive objects, and were able to identify and dismiss most naturally occurring radioactive material. However, as the amount of source material declined in size, the detection capabilities of both types of portal monitors converged. Because the data produced by the test runs is voluminous and complex, NIST and another contractor are still in the process of analyzing the test data and plan to produce a report summarizing the results of the testing in 2006. DNDO received responses to the Advanced Spectroscopic Portal Request for Proposal in February 2006, and intends to use the data from the Nevada Test Site to help evaluate these responses. In fiscal year

2006, DNDO also intends to award contracts to two or three manufacturers for further engineering development and production.

The second new technology is "high-Z detection," which is designed to better detect high atomic number (high-Z) materials—such as Special Nuclear Material (SNM)—and shielding materials—such as lead—that could be used to shield gamma radiation from portal monitors. The Cargo Advanced Automated Radiography System (CAARS) program within DNDO is intended to develop the technologies necessary for automated detection of high-Z material. DNDO envisions using the advanced portal monitor technology for the detection of lightly shielded nuclear threats and radiological dispersal devices, and using CAARS technology for the detection of high-Z materials.

The third new technology is "active interrogation," which is designed to better detect nuclear material, especially shielded sources, and DNDO expects it to play a role further in the future than advanced portal monitors and CAARS. DHS and DOE are supporting research at DOE national laboratories, such as Los Alamos and Lawrence Livermore, to develop these systems. Active interrogation systems probe or "interrogate" containers with neutron or gamma rays to induce additional radiation emissions from radioactive material within the container. According to DNDO, these systems are too large and costly to consider for current use. In addition, because these systems emit radiation, care will have to be taken to ensure personnel safety before any deployments are made.

In addition to these relatively near-term research and development efforts, DNDO intends to solicit proposals from private, public, academic, and federally funded research centers to pursue radiation detection projects with a more long-term orientation. The solicitation identifies five areas of research:

- mobile detection systems that can be used to detect potential radiological threats that are in transit, at fixed locations, and at special events;
- detection systems that can be integrated into ships, trucks, planes, or into containers;
- active detection technologies, including portal monitors and handheld devices that can detect and verify the presence of shielded nuclear materials;

- innovative detector materials that provide improved detection and isotope identification capabilities over existing materials, in addition to technologies that lead to reductions in the costs to manufacture detector materials, increasing the size and choice of the shapes of detector materials without a loss in performance; and
- alternate means to detect and identify nuclear material other than through radiation detection such as mass, density, or temperature.

DHS Sponsors Test Facilities in Nevada, New York, and New Jersey to Support Efforts to Improve Detection Capabilities

DHS is testing commercially available portal monitors, advanced portal monitors, and handheld devices at its new Radiological and Nuclear Countermeasures Test and Evaluation Complex at the Nevada Test Site (NTS). DNDO, with assistance from DOE's National Nuclear Security Administration, began construction of the complex in 2005.[21] While construction work is under way, an Interim Test Track was built nearby. The complex is to support the DNDO's development, testing, acquisition, and support of the deployment of radiation detection technologies. When completed, the complex will be comprised of several operating areas where testing and evaluation of detection systems will be conducted, such as a testing facility to evaluate active interrogation technologies; and a large, instrumented outdoor testing area to test mobile detection systems. The complex will also have a vehicle choke point where detection systems for land border crossings, toll plazas, and entrances to tunnels and bridges can be evaluated. According to DNDO officials, an important advantage of using NTS is that it provides the necessary facilities to test detection system capabilities with special nuclear materials in threat-representative configurations. The complex will be open to other organizations within DHS, including CBP, S&T, the Transportation Security Administration, and the U.S. Coast Guard. It will also be open to DOE national laboratories, universities, and private companies conducting radiation detection development and production for DHS. The facility is expected to become fully operational in January 2007.

In addition to the Nevada complex, DHS manages CMTB to test radiation detection equipment in an operational environment. The CMTB originated

[21]The National Nuclear Security Administration is a separately organized agency within DOE that was created by the National Defense Authorization Act for fiscal year 2000 with responsibility for the nation's nuclear weapons, nonproliferation, and naval reactors programs. Pub. L. No. 106-65 (1999).

as a DOE funded demonstration project in fiscal year 2003, but transferred to DHS in August 2003. The scientific, engineering, and technical staff of the CMTB are drawn predominantly from the national laboratories. The test bed encompasses various operational settings, such as major seaports, airports, roadways, and railways. The CMTB deploys commercially available and advanced radiation detection equipment at these venues to test and evaluate their performance in real-world situations, to develop better standard operating procedures, and to assess the impact the equipment has on the flow of commerce. At present, CMTB is testing portal monitors at toll crossings of two tunnels and one bridge, two seaport terminals, and two air cargo facilities. In addition, CMTB is developing several advanced secondary inspection mobile technologies. (See fig. 5.) The advanced spectroscopic portal monitors that DNDO is developing will likely be evaluated at the CMTB, once testing is completed at the Nevada Test Site.

Figure 5: The "SMARTCART," a Mobile Portal Monitor Using Advanced Detection Technology, Being Tested at the CMTB in New York

Source: GAO.

The Newly Created Domestic Nuclear Detection Office Is Structured to Improve Coordination of Executive Branch Radiation Detection Programs

DHS works with DOE, DOD, and other federal, state, and local agencies, as well as the private sector to carry out radiation detection programs. The newly established DNDO was set up to serve as DHS's main instrument for coordinating these efforts. Since its creation in April 2005, DNDO has entered into working relationships with other agencies and is taking the lead in developing what it calls a "global architecture," an integrated approach to detecting and stopping nuclear smuggling. However, because DNDO was created so recently, these efforts are in their early stages of development and implementation.

DNDO Attempts to Improve Cooperation Among Other DHS Offices, DOE, DOD, and Other Agencies in Deploying and Operating Equipment

Historically, cooperation among agencies engaged in domestic radiation detection has been limited. In April 2005, however, the president signed a joint presidential directive that directed the establishment of DNDO to, among other things, improve such cooperation by creating a single accountable organization with the responsibility for establishing strong linkages across the federal government and with other entities. As currently envisioned under the directive, DNDO's mission covers a broad spectrum of radiological and nuclear protective measures, but focuses mainly on nuclear detection. The directive includes several provisions directing DNDO to coordinate its activities with other entities. For example, DNDO is to work with DOE, DOD, the Departments of State and Justice, state and local agencies, and the private sector to develop programs to thwart illicit movements of nuclear materials. In addition, provisions of the directive require consultation between DNDO, law enforcement and nonproliferation centers, as well as other related federal and state agencies. Table 2 provides a summary of the cooperation brought about by the presidential directive.

Table 2: Cooperation with DNDO Brought about by Presidential Directive

Agency	Responsibilities
Department of Homeland Security	
S&T	All radiological/nuclear detection programs and staff subsumed by DNDO.
U.S. Coast Guard (USCG)	USCG and DNDO coordinate on detection and reporting resources, and protocols to ensure that USCG equipment is state-of-the-art and that detection events are properly reported.
Office of State & Local Government Coordination and Preparedness (SLGCP)	DNDO works to ensure good communication, coordination, and takes other actions with state and local governments. SLGCP personnel help staff DNDO.
Interagency Components	
Department of Energy	Provide staffing to, and coordinates with, DNDO in equipping National Incident Response Teams. DOE also provides DNDO with information from overseas programs. Makes the NTS and special nuclear materials available for DNDO testing.
Department of Defense	Provide staffing to DNDO. Facilitate coordination between DOD detection programs and domestic programs. Coordinate on technical "reachback capabilities." Integrate any domestic detection systems in communities near military bases with DNDO assets.
Department of Justice	Provide staffing to DNDO. FBI will coordinate on establishing and executing "reachback capabilities." FBI remains the lead law enforcement agency in terrorist events.
Department of State	Provide links and overall coordination between DNDO and non-U.S. organizations responsible for radiation detection.

(Continued From Previous Page)

Agency	Responsibilities
Central Intelligence Agency	Primary responsibility for gathering, analyzing, and disseminating intelligence information relevant to DNDO operations. The agency will accept collection requirements through channels from DNDO.
Nuclear Regulatory Commission	Coordinate detection requirements with DNDO. DNDO shares detection event data with NRC, and NRC shares information with DNDO on legal shipments of radiological materials.

Source: DNDO.

According to senior DNDO officials, although the close cooperation called for in DNDO's mandate has been difficult to achieve, there are two factors that may help DNDO succeed in this effort. First, the presidential directive is explicit in directing other federal agencies to support DNDO's efforts. The directive transfers primary responsibility for radiation and nuclear detection activities in the United States to DNDO, and requires DNDO to include personnel from other agencies in its organization. For example, under the directive, DOE will provide DNDO with information received from overseas programs, including the Megaports Initiative and others, as well as information from DOE's international partners involved with radiological and nuclear detection systems. Second, all of the radiological and nuclear detection programs and staff of S&T became part of DNDO.

DOE's Second Line of Defense program supports DNDO efforts by working with the agency to exchange information, data, and lessons learned from overseas deployments. According to senior officials at DNDO, the data from overseas deployments are needed to help DNDO efforts to develop profiles of potential risks to the United States. In addition, the performance of these systems, as evidenced by these data, can help improve domestic portal monitors' ability to detect radiation. In addition, DOE provides equipment training opportunities for DHS personnel. In April 2005, DOE and DHS formalized certain aspects of this cooperation in a memorandum of understanding. Specifically, the areas of cooperation include, among other things: discussing procedures for the rapid analysis of cargo and for operational/emergency responses, training CBP officers, exchanging technical and lessons learned information, and providing updates on their respective programs' implementation.

DHS has also entered into formal agreements with state and local governments to coordinate their radiation detection efforts. For example, in April 2005, just prior to DNDO's creation, DHS and the Port Authority of New York and New Jersey finalized a memorandum of understanding to provide services, personnel, and equipment to run the CMTB program.

Specifically, the program is designed to evaluate and assess the role of threat detection technologies, develop and exercise various concepts of operation and response tools, integrate lessons learned from field experiences, and provide detection and monitoring capabilities for testing and evaluation purposes. The agreement spells out each partner's responsibilities, including coordination with other agencies. According to a senior DNDO official, DNDO now has responsibility for this and other similar agreements under its authority to develop and evaluate new radiation detection equipment.

Finally, DNDO officials also believe that the way the agency has been staffed and organized will aid its cooperation efforts. For example, staff from DHS, DOD, DOE, the Departments of State and Justice, and other agencies, have been detailed to DNDO. All of DNDO's major organizational units are staffed with personnel from multiple agencies. For example, the strategic planning staff within the Office of the Director has employees from DOE, DOD, CBP, Federal Bureau of Investigation (FBI), and DHS's Office of State and Local Government Coordination and Preparedness. Significantly, DNDO's Office of Operations Support, which is designed to provide real-time situational data as well as technical support to field units, is headed by an FBI executive with senior staff from CBP, DOE, and DHS's Transportation Security Administration providing direct management support. According to a senior DNDO official, having this broad range of agencies represented in DNDO decision making helps ensure that agencies' views are heard and fully considered, thereby helping to achieve the greatest possible consensus even for difficult decisions. Further, agency personnel detailed to DNDO have the authority to "bind" their respective agencies, i.e., whatever decisions or agreements are reached under the auspices of DNDO will bind their agency to comply to the extent permitted by law. Finally, according to senior officials in DOE and CBP, the current organizational arrangement appears to be working. Officials noted that early in DNDO's history, communication was difficult, but has recently improved. For example, CBP and DOE officials told us they had hoped to have greater input into DNDO's early efforts to develop integrated radiation detection systems. However, these officials noted that by October 2005, DNDO seemed to have heard and acted upon their recommendations. However, although these officials were optimistic about future collaborations with DNDO, they also noted that DNDO has not yet completed a large enough body of work to conclude firmly that its coordination efforts will always be similarly successful.

DNDO Is Cooperating with Other Agencies to Develop a Global Nuclear Detection System

Among the main purposes in creating the DNDO, according to its Director, is to develop a global nuclear detection system that he characterized as a "global architecture." DNDO's intention in developing such an approach is to coordinate other agencies' efforts, such as the Second Line of Defense and Container Security Initiative, with the domestic deployment program to create an integrated, worldwide system. The resulting "global architecture" would be a multi-layered defense strategy that includes programs that attempt to secure nuclear materials and detect their movements overseas; to develop intelligence information on nuclear materials' trans-shipments and possible movement to the United States; and to integrate these elements with domestic efforts undertaken by governments—federal, state, local, and tribal—and the private sector. Much of DNDO's work in terms of acquiring and supporting the deployment of radiation detection equipment, as well as in supporting research, development, and testing of new detection equipment supports the office's mission to develop the U.S. domestic portion this global architecture.

In addition, DHS, in conjunction with selected state and local organizations, as well as other federal agencies and the private sector, began two pilot projects in fiscal year 2003 to demonstrate a layered defense system designed to protect the United States against radiological and nuclear threats. DHS's Radiological Pilot Programs Office coordinated the projects' initial efforts, and DNDO assumed responsibility in October 2005. Field work began in fiscal year 2004 and will be completed in fiscal year 2007. The project leaders expect the final report and lessons learned to be issued in fiscal year 2007. Both pilot projects featured a broad selection of federal, state, and local agencies, including state law enforcement, counter-terrorism, emergency management, transportation, and port authorities.

Conclusions

DHS has made progress deploying radiation detection equipment at U.S. ports-of-entry; notably, the department achieved these gains without greatly impeding the flow of commerce (i.e., the movement of cargo containers out of ports-of-entry). However, we believe that DHS will find it difficult under current plans and assumptions to meet its current portal monitor deployment schedule at U.S. borders because it would have to increase its current rate of deployment by 230 percent to meet its September 2009 deadline. Our analysis of CBP's and PNNL's earned value data suggests that millions of dollars worth of work is being deferred each month and that the work that is completed is costing millions more than

planned. Currently, we estimate that CBP is facing a likely cost overrun of about $340 million, and that the last portal monitor may not be installed until late 2014. Unless CBP and PNNL make immediate improvements in the schedule performance, then additional slippage in the deployment schedule is likely.

A key overriding cause for these delays is the late disbursal of funds to DHS contractors. This late dispersal disrupts and delays some ongoing installation projects. In this regard, DHS approval processes for documentation requested by the House Appropriations Committee are lengthy and cumbersome. In one case, for example, funds for fiscal year 2005 were not made available to the DHS contractor until September 2005, the last month of the fiscal year. This process is taking too long and needs to be shortened.

Further, the unsure efficacy and uncertain cost associated with the advanced portal monitor technology means that DHS cannot determine, with confidence, how much the program will eventually cost. In particular, even if the advanced portal monitor technology can be shown superior to current technology—which currently does not seem certain—DHS does not yet know whether the new technology will be worth its considerable additional cost. Only after testing of the advanced portal monitors has been completed and DHS has rigorously compared currently-fielded and advanced portal monitors, taking into account their differences in cost, will DHS be able to answer this question.

CBP has experienced difficulty deploying portal monitors at seaports, at least in part because it has been unable to reach agreements with many seaport operators, who are concerned that radiation detection efforts may delay the flow of commerce through their ports. As a result, the agency has fallen 2 years behind its seaport deployment schedule—and seaports continue to be vulnerable to nuclear smuggling. Significantly, there is no clear solution and no reason to be optimistic that progress can be made soon. CBP's policy of negotiating deployment agreements with seaport terminal operators has not yet yielded agreements at many seaports and this has caused significant delays in the deployment of portal monitors at some seaports. CBP has chosen not to attempt to force terminal operators to cooperate. A subset of this issue concerns screening rail traffic leaving seaports, which is a particularly difficult problem. The operational concerns of performing secondary rail inspections in seaports are daunting. Some port operators as well as a national study strongly suggest that rail transport will increase over the next 10 years. However, unless an

effective and efficient means to screen rail traffic is developed and deployed, seaports will likely continue to either avoid installing detection equipment altogether, or simply turn it off when its operation might prove to be inconvenient. Without more progress on this front, we risk rail cargo becoming a burgeoning gap in our defenses against nuclear terrorism.

CBP appears to have made progress in using radiation detection equipment correctly and adhering to inspection procedures. At several ports-of-entry we visited, CBP officers physically opened and inspected cargo containers to confirm the nature of the radiological source under certain circumstances. They did this when they were unable to confirm the type of radiological material through current approved procedures. Since the currently deployed handheld equipment is limited in its ability to accurately identify sources of radiation, opening the container allows CBP officers to get closer to the source of the alarm and thereby improve their chances of accurately identifying the source. It also enables officers to verify that the container's contents are consistent with the isotope identifier's initial reading and the container's manifest. Furthermore, since DHS and DOE officials have expressed concerns that illicit radiological material could be shielded, this practice enables officers to conduct a more thorough examination of the containers' contents—thereby increasing the likelihood that CBP officers will find any illicit radioactive material. Importantly, this process, according to border security officials, did not impede the progress of commerce through any port-of-entry.

On the other hand, because CBP officers do not have access to NRC licensing data, it is difficult for them to verify that shippers have obtained necessary NRC licenses and to verify the authenticity of any NRC licenses that may accompany shipments of radioactive materials. As a result, unless nuclear smugglers in possession of faked license documents raised suspicions in some other way, CBP officers could follow agency guidelines yet unwittingly allow them to enter the country with their illegal nuclear cargo. As we see it, this is a significant gap in CBP's national procedures that should be closed.

Recommendations for Executive Action

Since DHS provides the Congress with information concerning the acquisition and deployment of portal monitors, and since DHS's procedures to obtain internal agreement on this information are lengthy and cumbersome—often resulting in delays—we recommend that the Secretary of Homeland Security, working with the Director of DNDO and the Commissioner of CBP, review these approval procedures and take actions

necessary to ensure that DHS submits information to the Congress early in the fiscal year.

In order to complete the radiation portal monitor deployment program, as planned, we recommend that the Secretary of Homeland Security, working with the Director of DNDO, and in concert with CBP and PNNL, devise a plan to close the gap between the current deployment rate and the rate needed to complete deployments by September 2009.

To ensure that DHS's substantial investment in radiation detection technology yields the greatest possible level of detection capability at the lowest possible cost, we recommend that once the costs and capabilities of advanced technology portal monitors are well understood, and before any of the new equipment is purchased, the Secretary of Homeland Security work with the Director of DNDO to analyze the benefits and costs of deploying advanced portal monitors. This analysis should focus on determining whether any additional detection capability provided by the advanced equipment is worth its additional cost. After completing this cost-benefit analysis, the Secretary of Homeland Security, working with the Director of DNDO, should revise its total program cost estimates to reflect current decisions.

To help speed seaport deployments and to help ensure that future rail deployments proceed on time, we recommend that the Secretary of Homeland Security, in cooperation with the Commissioner of CBP, develop procedures for effectively screening rail containers and develop new technologies to facilitate inspections.

To increase the chances that CBP officers find illicit radiological material, we recommend that the Secretary of Homeland Security, working with the Commissioner of CBP, consider modifying the agency's standard operating procedures for secondary inspections to include physically opening cargo containers during secondary inspections at all ports-of-entry when the external inspection does not conclusively identify the radiological material inside.

To further increase the chances that CBP officers identify illicit radiological material, we recommend that the Secretary of Homeland Security, working with the Chairman of NRC, develop a way for CBP border officers to determine whether radiological shipments have the necessary NRC licenses and to verify the authenticity of NRC licenses that accompany such shipments.

To ensure that CBP is receiving reliable cost and schedule data, we recommend that the Secretary of Homeland Security direct PNNL to have its earned value management system validated so that it complies with guidance developed by the American National Standards Institute/ Electronic Industries Alliance. In addition, we recommend the Secretary of Homeland Security direct CBP and PNNL to conduct an Integrated Baseline Review to ensure its earned value management data is reliable for assessing risk and developing alternatives.

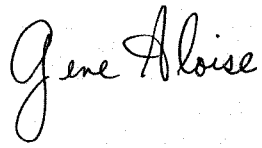
Agency Comments and Our Evaluation

We provided a draft of this report to DHS for comment. In response, we received written comments from DHS officials. DHS noted that the report is factually correct. Further, the Department agreed with our recommendations and committed to implementing them. DHS officials also commented that our review did not completely capture the enormity or complexity of the Radiation Portal Monitor program. We agree that this program is a massive undertaking, and our original draft reflected this perspective in several places. In commenting on our recommendation to develop a better means for CBP border officers to verify NRC license information, DHS stated that "NRC licenses are required to accompany certain legitimate shipments of radiological materials..." However, according to senior NRC officials, no requirement that the license accompany the shipment exists. Finally, DHS provided some clarifying comments that we incorporated into this report, as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the congressional committees with jurisdiction over DHS and its activities; the Secretary of Homeland Security; the Director of OMB; and interested congressional committees. We will also make copies of the report available to others upon request. This report will also be available at no charge on GAO's home page at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3841. Contact points for our Offices of Congressional Relations

and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



Gene Aloise
Director, Natural Resources and Environment

List of Requesters

The Honorable Norm Coleman
Chairman
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Carl Levin
Ranking Minority Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Appendix I

Scope and Methodology

To assess the Department of Homeland Security's (DHS) progress in deploying radiation detection equipment, including radiation portal monitors, radiation isotope identification devices, and pagers at U.S. ports-of-entry and any problems associated with that deployment, we reviewed documents and interviewed officials from the U.S. Customs and Border Protection (CBP), Domestic Nuclear Detection Office (DNDO), and Pacific Northwest National Laboratory (PNNL). We focused primarily on the issues surrounding radiation portal monitors because they are a major tool in the federal government's efforts to thwart nuclear smuggling, and because the budget and other resources devoted to these machines far exceeds the handheld equipment also used at U.S. ports-of-entry. Further, we focused on the use of radiation detection equipment in primary and secondary inspections, but we did not examine their use as a part of CBP's targeted inspections. To assess CBP's current progress in deploying portal monitors, we compared PNNL's December 2004 project execution plan for deploying radiation portal monitors—including the project's schedule and estimated cost. We analyzed budget, cost, and deployment data on portal monitors to determine differences between PNNL's plan and its current progress. We also assessed PNNL's cost and schedule performance using earned value analysis techniques based on data captured in PNNL's contract performance reports. We also developed a forecast of future cost growth. We based the lower end of our forecast range on the sum of costs spent to date and the forecast cost of work remaining. The remaining work was forecast using an average of the current cost performance index efficiency factor. For the upper end of our cost range, we relied on the actual costs spent to date added to the forecast of remaining work with an average monthly cost and schedule performance index.

We also visited a nonprobability sample of CBP ports-of-entry, including two international mail and express courier facilities, five seaports, and three land border crossings.[1] We selected these ports-of-entry by using criteria such as the types of ports-of-entry where CBP plans to deploy equipment; ports-of-entry with wide geographic coverage; and ports-of-entry where portal monitors have been—or are planned to be—installed. During each visit, we spoke with CBP inspectors and local port authority officials on the progress made, and any problems experienced in deploying the equipment at their locations.

[1]Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample, some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

To assess CBP officers' use of radiation detection equipment, and how inspection procedures are implemented at U.S. ports-of-entry, and any problems associated with the use of the equipment, we reviewed CBP's standard operating procedures for radiation detection; documents on its training curriculum; and training materials on how to use the equipment. We participated in a 3-day hands-on training course for CBP officers at PNNL on how to use radiation detection equipment. We also interviewed officials from CBP field and headquarters to discuss problems associated with the use of the equipment. During our site visits, we toured the facilities, observed the equipment in use, and interviewed CBP officers about radiation detection policies and procedures and the deployment of equipment at their locations. We discussed with CBP officers how they determine the validity of Nuclear Regulatory Commission (NRC) licenses when legitimate shipments of radioactive material enter the nation.

To assess DHS's progress in improving and testing radiation detection equipment capabilities, we reviewed documents and interviewed officials from CBP, DNDO, Science and Technology Directorate (S&T), DOE, PNNL, and the National Institute for Standards and Technology (NIST). We reviewed S&T's April 2005 Program Execution Plan; DHS documentation on the development of advanced radiation detection technologies; and test results and assessments of the performance of both commercially available radiation detection equipment and advanced technologies. We visited four national laboratories—Lawrence Livermore, Los Alamos, Pacific Northwest, and Sandia—that are involved in the research, development, and testing of radiation detection technologies. In addition, we visited the Counter Measures Test Bed (CMTB) in New York and New Jersey, the Nevada Test Site, and the Department of Defense's (DOD) test site at a U.S. Air Force base to observe the testing of radiation detection equipment and discuss progress in improving and testing radiation detection equipment with onsite experts.

To assess the level of cooperation between DHS and other federal agencies in conducting radiation detection programs, we interviewed officials from CBP; S&T; the Transportation Security Administration; DOD's Defense Threat Reduction Agency; DOE's National Nuclear Security Administration; and Lawrence Livermore, Los Alamos, Pacific Northwest, and Sandia National Laboratories. We discussed the current extent of coordination and whether more coordination could result in improvements to DHS's deployment, development, and testing of radiation detection equipment and technologies. We reviewed agency agreements to cooperate, including a memorandum of understanding between DHS and DOE to exchange

information on radiation detection technologies and deployments, and a memorandum of understanding between DHS and the Port Authority of New York and New Jersey to integrate lessons learned into domestic radiation detection efforts. In addition, we reviewed an organizational chart from DNDO as well as our past reports on coordination between federal agencies on deployment and testing.

We received training data from CBP, cost and budget data from CBP, and deployment data from CBP and PNNL. We obtained responses from key database officials to a number of questions focused on data reliability covering issues such as data entry access, internal control procedures, and the accuracy and completeness of the data. We determined these data were sufficiently reliable for the purposes of this report.

We conducted our review from March 2005 to February 2006 in accordance with generally accepted government auditing standards.

Appendix II

GAO Contact and Staff knowledgments

GAO Contact

Gene Aloise, (202) 512-3841

Acknowledgments

In addition to the contact named above, Jim Shafer; Nancy Crothers; Emily Gupta; Brandon Haller; Richard Hung; Winston Le; Greg Marchand; Judy Pagano; Karen Richey; Keith Rhodes, GAO's Chief Technologist; and Eugene Wisnoski made key contributions to this report.

Related GAO Products

Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries. GAO-06-311. Washington, D.C.: March 14, 2006.

Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and in Other Countries. GAO-05-840T. Washington, D.C.: June 21, 2005.

Homeland Security: Key Cargo Security Programs Can Be Improved. GAO-05-466T. Washington, D.C.: May 25, 2005.

Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts. GAO-05-557. Washington, D.C.: April 26, 2005.

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. GAO-05-375. Washington, D.C.: March 31, 2005.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Nuclear Nonproliferation: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning. GAO-02-426. Washington, D.C.: May 16, 2002.

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

April 10, 2006

ERRATA

Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation's Borders at Selected Locations (GAO 06-545R, March 28, 2006).

GAO reposted the Web version of this report on April 10, 2006, to reflect changes in the text on pages 2 and 8. The original version of the report, posted on March 28, implied that officials from the National Institute of Standards and Technology selected the amount of radioactive sources we used in our border testing. The reposted version clarifies that GAO determined the amount of radioactive sources used in the tests after consulting with an outside expert.

Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

March 28, 2006

The Honorable Norm Coleman
Chairman
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Chairman:

Subject: *Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation's Borders at Selected Locations*

This report responds to your request that we investigate potential security weaknesses related to the installation of radiation detection equipment at U.S. ports of entry. Based on discussions with your staff, we focused our efforts on testing whether the radiation portal monitors installed at the U.S. ports of entry would detect radioactive material transported in vehicles attempting to enter the United States. We also agreed to provide our observations regarding the procedures that Department of Homeland Security U.S. Customs and Border Protection (CBP) inspectors followed when the radiation portal monitors detected such material.

We have reported on the security of our nation's northern border in terms of detection of illegal transport of radioactive material into the United States in our previous work.

Scope and Methodology

We selected two land ports of entry that had radiation portal monitors installed: one at the U.S.-Canadian border and one at the U.S.-Mexican border. Radiation portal monitors are large pieces of stationary equipment that CBP uses as part of its overall strategy to thwart radiological terrorism by detecting the presence of radioactive materials by screening people, vehicles, and cargo as they pass through ports of entry. In order to safely plan and execute our undercover operation, several of our investigators attended training at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland. Our investigators received training on the safe handling, storage, and transport of radioactive materials.

When considering the type of radioactive sources to use in our undercover operation, we decided to use one of the most common radioisotopes used in industry for its strong radioactivity. After consulting with an outside expert, we used an amount of radioactive sources that we determined was sufficient to manufacture a dirty bomb.[1]

As part of our investigation, we purchased a small quantity of the radioactive sources from a commercial source by posing as an employee of a fictitious company. This was to demonstrate that anyone can purchase small quantities of radioactive sources for stockpiling because suppliers are not required to exercise any due diligence in determining whether the buyer has a legitimate use for the radioactive sources and suppliers are not required to ask the buyer to produce a Nuclear Regulatory Commission (NRC) document when making purchases in small quantities. We then deployed two teams of investigators to the field to make simultaneous border crossings at the northern and southern borders in an attempt to transport radioactive sources into the United States.

While making our simultaneous crossings, we focused our investigation on whether the radiation portal monitors would detect the radioactive sources we carried and whether CBP inspectors exercised due diligence to determine the authenticity of paperwork presented by individuals attempting to transport radioactive sources across our borders. Although we offer observations on the procedures that CBP inspectors followed for our two border crossings, we did not evaluate the adequacy of the design or effectiveness of those procedures. Our investigation also tested whether an NRC document could be counterfeited using data easily accessible and available to the public. We conducted our investigation from July 2005 through December 2005 in accordance with quality standards for investigations as set forth by the President's Council on Integrity and Efficiency.

Summary of Investigation

For the purposes of this undercover investigation, we purchased a small amount of radioactive sources and one container used to store and transport the material from a commercial source over the telephone. One of our investigators, posing as an employee of a fictitious company located in Washington, D.C., stated that the purpose of his purchase was to use the radioactive sources to calibrate personal radiation detection pagers. The purchase was not challenged because suppliers are not required to determine whether buyers have legitimate uses for the radioactive sources, nor are suppliers required to ask the buyer to produce an NRC document when making purchases in small quantities.

[1] According to the Centers for Disease Control and Prevention, a dirty bomb is a mix of explosives, such as dynamite, with radioactive powder or pellets. When the dynamite or other explosives are set off, the blast carries radioactive material into the surrounding area.

The radiation portal monitors properly signaled the presence of radioactive material when our two teams of investigators conducted simultaneous border crossings. Our investigators' vehicles were inspected in accordance with most of the CBP policy at both the northern and southern borders. However, our investigators were able to enter the United States with enough radioactive sources to make two dirty bombs using counterfeit documents. Specifically, they were able to successfully represent themselves as employees of a fictitious company and present a counterfeit bill of lading and a counterfeit NRC document during the secondary inspections at both locations. The CBP inspectors never questioned the authenticity of the investigators' counterfeit bill of lading or the counterfeit NRC document authorizing them to receive, acquire, possess, and transfer radioactive sources.

Background

A dirty bomb, or a radiological dispersal device, combines a conventional explosive with radioactive material. In most cases, the conventional explosive would have more immediate lethality than the radioactive material. A dirty bomb would most likely result in small radiation exposures and would typically not contain enough radiation to kill people or cause severe illnesses. However, by scattering the radioactive material, the dirty bomb has the effect of contaminating an area. The extent of local contamination depends on several factors, including the size of the explosive, the amount and type of radioactive material used, and weather conditions. While there could be an increase in the cancer risk among those exposed to radiation from a dirty bomb, the more significant effect of a dirty bomb could be the closing of contaminated areas. The direct costs of cleanup and the indirect losses in trade and business in the contaminated areas could be large. Hence, dirty bombs are generally considered to be weapons of mass disruption instead of weapons of mass destruction.

Many radioactive materials are used in a variety of industrial, scientific, and medical applications. For instance, radioactive materials are used in smoke detectors and for cancer treatments. However, few of the materials are considered suitable for use in a dirty bomb. A Department of Energy and Nuclear Regulatory Commission Interagency Working Group identified radioactive materials of highest concern based on the potential dose impacts of the materials and the availability of such materials in sufficient quantities.[2]

To address the threat of dirty bombs and other nuclear material, the federal government has programs in place that regulate the transportation of radioactive material and to prevent illegal transport of radioactive material across our nation's borders. CBP uses radiation detection equipment at ports of entry to prevent the illicit transport of radioactive material into the United States. The goal of CBP's inspection program is to "...thwart the operations of terrorist organizations by

[2] Department of Energy/Nuclear Regulatory Commission Interagency Working Group on Radiological Dispersion Devices. *Radiological Dispersal Devices: An Initial Study to Identify Radioactive Materials of Greatest Concern and Approaches to Their Tracking, Tagging, and Disposition*, Report to the Nuclear Regulatory Commission and the Secretary of Energy (May 2003).

detecting, disrupting, and preventing the cross-border travel of terrorists, terrorist funding, and terrorist implements, including Weapons of Mass Destruction and their precursors." Deploying radiation detection equipment is part of CBP's strategy for thwarting radiological terrorism and CBP is using a range of such equipment to meet its goal of screening all cargo, vehicles, and individuals coming into the United States.

Most travelers enter the United States through the nation's 154 land border ports of entry. CBP inspectors at ports of entry are responsible for the primary inspection of travelers to determine their admissibility into the United States and to enforce laws related to preventing the entry of contraband, such as drugs and weapons of mass destruction.

Radiation Detection Devices

To help detect the presence of radiation and identify the type of radiation present, CBP generally relies on three types of radiation detection devices – radiation portal monitors, Personal Radiation Detectors (PRDs), and Radiation Isotope Identifier Devices (RIIDs). Radiation portal monitors have the ability to detect the presence of gamma radiation, which is emitted by all radioactive materials of greatest concern,[3] and neutrons, which are emitted by only a limited number of materials, including plutonium. CBP uses PRDs that detect the presence of gamma radiation but not neutrons. CBP requires its inspectors to wear PRDs while on duty and ensure that the PRDs are activated. PRDs alert inspectors to the presence of harmful levels of radiation when they are conducting cargo and vehicle searches. PRDs can detect radioactive materials that could be used in a radiological dispersal device, also known as a dirty bomb. Another type of radiation detection equipment that CBP uses are RIIDs, which are handheld devices designed to determine the identity of the radioactive material, whether it is a radiological source used in medicine or industry, a naturally occurring source of radiation, or weapons-usable nuclear material.

Radiation Detection Alerts

For the purposes of this report, we focused only on the procedures for gamma radiation, the type of radiation used in our tests. To identify the type of radiation present, inspectors use a handheld RIID. If the radiation portal monitor and the RIID do not detect the presence of neutrons, inspectors follow gamma radiation procedures, which require that they first use their PRDs to determine the safe distance at which to conduct an inspection.

If, after reviewing documentation or obtaining advice from Laboratories and Scientific Services personnel, the CBP inspectors are satisfied that the radioactive source is properly documented or is consistent with innocent radiation sources, the vehicle and passengers can be released. If CBP inspectors are not satisfied that the

[3] Radioactive materials of greatest concern are those materials that could be used in a nuclear weapon such as plutonium and highly enriched uranium.

source is documented or innocent, they must obtain guidance from the Laboratory and Scientific Services.

Documentation Was Produced to Support Undercover Investigation

As part of our undercover investigation, we produced counterfeit documents before sending our two teams of investigators out to the field. We found two NRC documents and a few examples of the documents by searching the Internet.[4] We subsequently used commercial, off-the-shelf computer software to produce two counterfeit NRC documents authorizing the individual to receive, acquire, possess, and transfer radioactive sources.

To support our investigators' purported reason for having radioactive sources in their possession when making their simultaneous border crossings, a GAO graphic artist designed a logo for our fictitious company and produced a bill of lading using computer software.

With Ease, Investigators Purchased, Received, and Transported Radioactive Sources across Both Borders

Our two teams of investigators each transported an amount of radioactive sources sufficient to manufacture a dirty bomb when making their recent, simultaneous border crossings. In our earlier work, we had purchased radioactive sources, two containers to store and transport the material, and we had obtained a genuine NRC document.

For the purposes of our current undercover investigation, we purchased a small amount of radioactive sources and one container for storing and transporting the material from a commercial source over the telephone. One of our investigators, posing as an employee of a fictitious company, stated that the purpose of his purchase was to use the radioactive sources to calibrate personal radiation detectors. According to the NRC, suppliers are not required to determine whether the buyer has a legitimate use for the radioactive sources, nor are suppliers required to ask the buyer to produce an NRC document when making purchases in small quantities. The amount of radioactive sources our investigator sought to purchase did not require an NRC document. The company mailed the radioactive sources to an address in Washington, D.C. We could have purchased all of the radioactive sources used in our two undercover border crossings by making multiple purchases from different suppliers, using similarly convincing cover stories, using false identities, and had all of the radioactive sources conveniently shipped to our nation's capital.

[4] None of these documents were available on NRC's Web site.

We have pointed out the weaknesses in federal and state controls over the security[5] of sealed sources in our prior work,[6] noting that it is possible that these materials can be obtained for malicious intent. Sealed radioactive sources, radioactive material encapsulated in stainless steel or other metal, are used worldwide in medicine, industry, and research. We recommended in August 2003 that NRC modify its process of issuing specific licenses to ensure that sealed sources cannot be purchased before NRC's verification – through inspection or other means – that the materials will be used as intended. NRC has not implemented our licensing recommendation to date, more than 2 years later. However, NRC has recently established an interagency task force to evaluate the licensing, use, and security of radioactive materials. Further delays in implementing our licensing recommendation, given today's security environment, continues to leave NRC's licensing process vulnerable to compromise and inadequate in terms of precluding the smuggling of radioactive material across our nation's borders.

Two Teams of Investigators Conducted Simultaneous Crossings at the U.S.-Canadian Border and U.S.-Mexican Border

Northern Border Crossing

On December 14, 2005, our investigators placed two containers of radioactive sources into the trunk of their rental vehicle. Our investigators – acting in an undercover capacity – drove to an official port of entry between Canada and the United States. They also had in their possession a counterfeit bill of lading in the name of a fictitious company and a counterfeit NRC document.

At the primary checkpoint, our investigators were signaled to drive through the radiation portal monitors and to meet the CBP inspector at the booth for their primary inspection. As our investigators drove past the radiation portal monitors and approached the primary checkpoint booth, they observed the CBP inspector look down and reach to his right side of his booth. Our investigators assumed that the radiation portal monitors had activated and signaled the presence of radioactive sources. The CBP inspector asked our investigators for identification and asked them where they lived. One of our investigators on the two-man undercover team handed the CBP inspector both of their passports and told him that he lived in Maryland while the second investigator told the CBP inspector that he lived in Virginia.

The CBP inspector also asked our investigators to identify what they were transporting in their vehicle. One of our investigators told the CBP inspector that they were transporting specialized equipment back to the United States. A second CBP inspector, who had come over to assist the first inspector, asked what else our

[5] As used in this report, "security" refers to measures to prevent unauthorized access to, loss, and/or theft of sealed sources, or radioactive materials used for medical and industrial purposes. See GAO, *Nuclear Security: Federal and State Action Needed to Improve Security of Sealed Radioactive Sources*, GAO-03-804 (Washington, D.C.: August 6, 2003).

[6] GAO-03-804.

investigators were transporting. One of our investigators told the CBP inspectors that they were transporting radioactive sources for the specialized equipment. The CBP inspector in the primary checkpoint booth appeared to be writing down the information. Our investigators were then directed to park in a secondary inspection zone, while the CBP inspector conducted further inspections of the vehicle.

During the secondary inspection, our investigators told the CBP inspector that they had an NRC document and a bill of lading for the radioactive sources. The CBP inspector asked if he could make copies of our investigators' counterfeit bill of lading on letterhead stationery as well as their counterfeit NRC document. Although the CBP inspector took the documents to the copier, our investigators did not observe him retrieving any copies from the copier.

Our investigators watched the CBP inspector use a RIID, which he said is used to identify the source of radioactive material, to examine the investigators' vehicle. He used the RIID to identify the source of radiation emanating from the investigators' vehicle. He told our investigators that he had to perform additional inspections. After determining that the investigators were not transporting additional sources of radiation, the CBP inspector made copies of our investigators' drivers' licenses, returned their drivers' licenses to them, and our investigators were then allowed to enter the United States. At no time did the CBP inspector question the validity of the counterfeit bill of lading or the counterfeit NRC document.

Southern Border Crossing

On December 14, 2005, our investigators placed two containers of radioactive sources into the trunk of their vehicle. Our investigators drove to an official port of entry at the southern border. They also had in their possession a counterfeit bill of lading in the name of a fictitious company and a counterfeit NRC document.

At the primary checkpoint, our two-person undercover team was signaled to drive through the radiation portal monitors through the use of a traffic light signal and stopped at the primary checkpoint for their primary inspection. As our investigators drove past the portal monitors and approached the primary checkpoint, they observed that the CBP inspector remained in the primary checkpoint for several moments prior to approaching our investigators' vehicle. Our investigators assumed that the radiation portal monitors had activated and signaled the presence of radioactive sources.

The CBP inspector asked our investigators for identification and asked them if they were American citizens. Our investigators told the CBP inspector that they were both American citizens and handed him their state issued driver's licenses. The CBP inspector also asked our investigators about the purpose of their trip to Mexico and asked whether they were bringing anything into the United States from Mexico. Our investigators told the CBP inspector that they were returning from a business trip in Mexico and were not bringing anything into the United States from Mexico.

While our investigators remained inside their vehicle, the CBP inspector used what appeared to be a RIID to scan the outside of the vehicle. One of our investigators told

him that they were transporting specialized equipment. The CBP inspector asked one of our investigators to open the trunk of the rental vehicle and to show him the specialized equipment. Our investigator told the CBP inspector that they were transporting radioactive sources in addition to the specialized equipment. The primary CBP inspector then directed our investigators to park in a secondary inspection zone for further inspection.

During the secondary inspection, the CBP inspector said he needed to verify the type of material our investigators were transporting, and another CBP inspector approached with what appeared to be a RIID to scan the cardboard boxes where the radioactive sources was placed. The instrumentation confirmed the presence of radioactive sources.

When asked again about the purpose of their visit to Mexico, one of our investigators told the CBP inspector that they had used the radioactive sources in a demonstration designed to secure additional business for their company. The CBP inspector asked for paperwork authorizing them to transport the equipment to Mexico. One of our investigators provided the counterfeit bill of lading on letterhead stationery, as well as their counterfeit NRC document. The CBP inspector took the paperwork provided by our investigators and walked into the CBP station. He returned several minutes later and returned the paperwork. At no time did the CBP inspector question the validity of the counterfeit bill of lading or the counterfeit NRC document.

Corrective Action Briefings

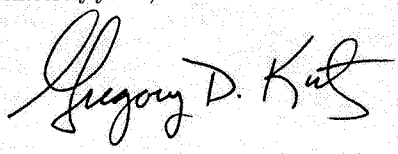
We conducted corrective action briefings with CBP officials and NRC officials shortly after completing our undercover operations. On December 21, 2005, we briefed CBP officials about the results of our border crossing tests. CBP officials agreed to work with the NRC and CBP's Laboratories and Scientific Services to come up with a way to verify the authenticity of NRC materials documents.

We conducted two corrective action briefings with NRC officials on January 12 and January 24, 2006, about the results of our border crossing tests. NRC officials disagreed with the amount of radioactive material we determined was needed to produce a dirty bomb, noting that NRC's "concern threshold" is significantly higher. We continue to believe that our purchase of radioactive sources and our ability to counterfeit an NRC document are matters that NRC should address. Further, we believe that the amount of radioactive sources that we were able to transport into the United States during our operation would be sufficient to produce two dirty bombs, which could be used as weapons of mass disruption. Finally, NRC officials told us that they are aware of the potential problems of counterfeiting documents and that they are working to resolve these issues.

As agreed with your office, unless you announce the contents of this report earlier, we will not distribute it until 30 days after its issuance date. At that time, we will send it to the appropriate congressional committees. We will also provide copies to the Department of Homeland Security and the Nuclear Regulatory Commission. If you or your staff have any questions regarding this report, please contact me at (202) 512-7455 (kutzg@gao.gov). Contact points for our Offices of Congressional Relations

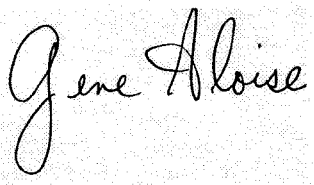
and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in enclosure I.

Sincerely yours,



Gregory D. Kutz
Managing Director
Forensic Audits
and Special Investigations

Keith A. Rhodes
Chief Technologist
Center for Technology
and Engineering



Gene Aloise
Director
Natural Resources
And Environment

Enclosure – 1

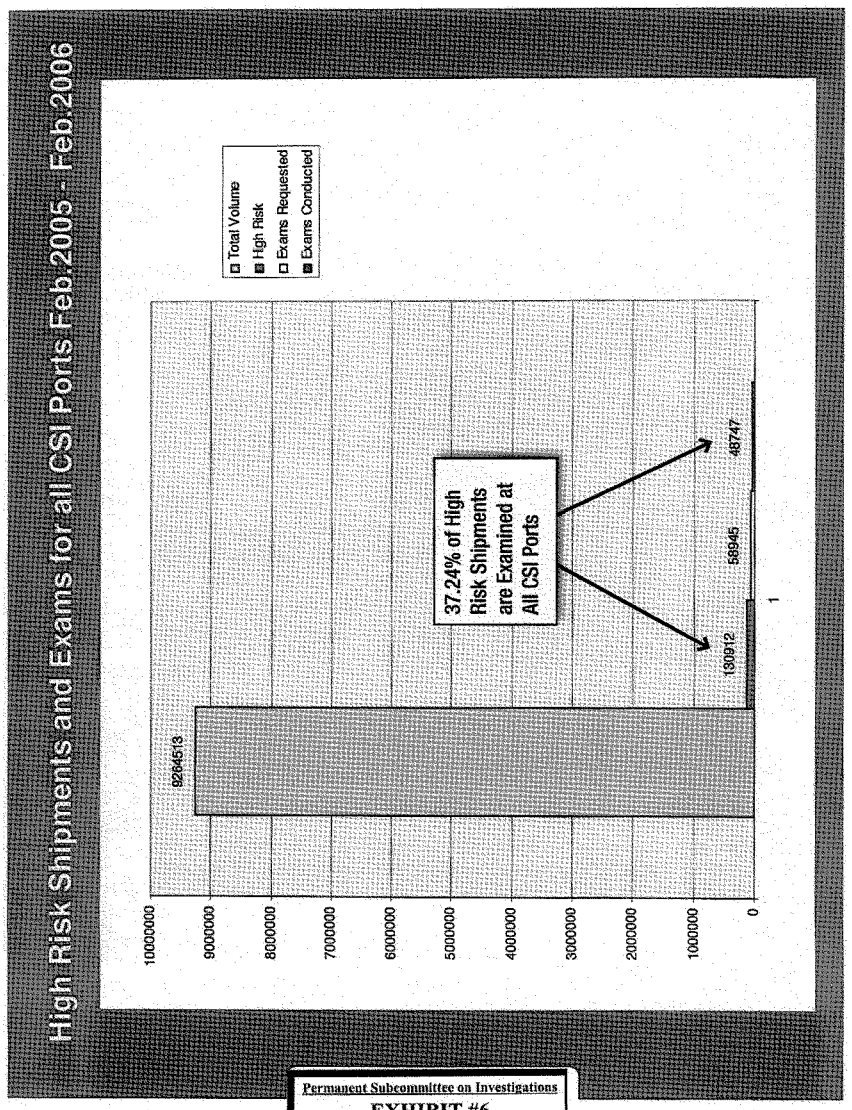
Enclosure I

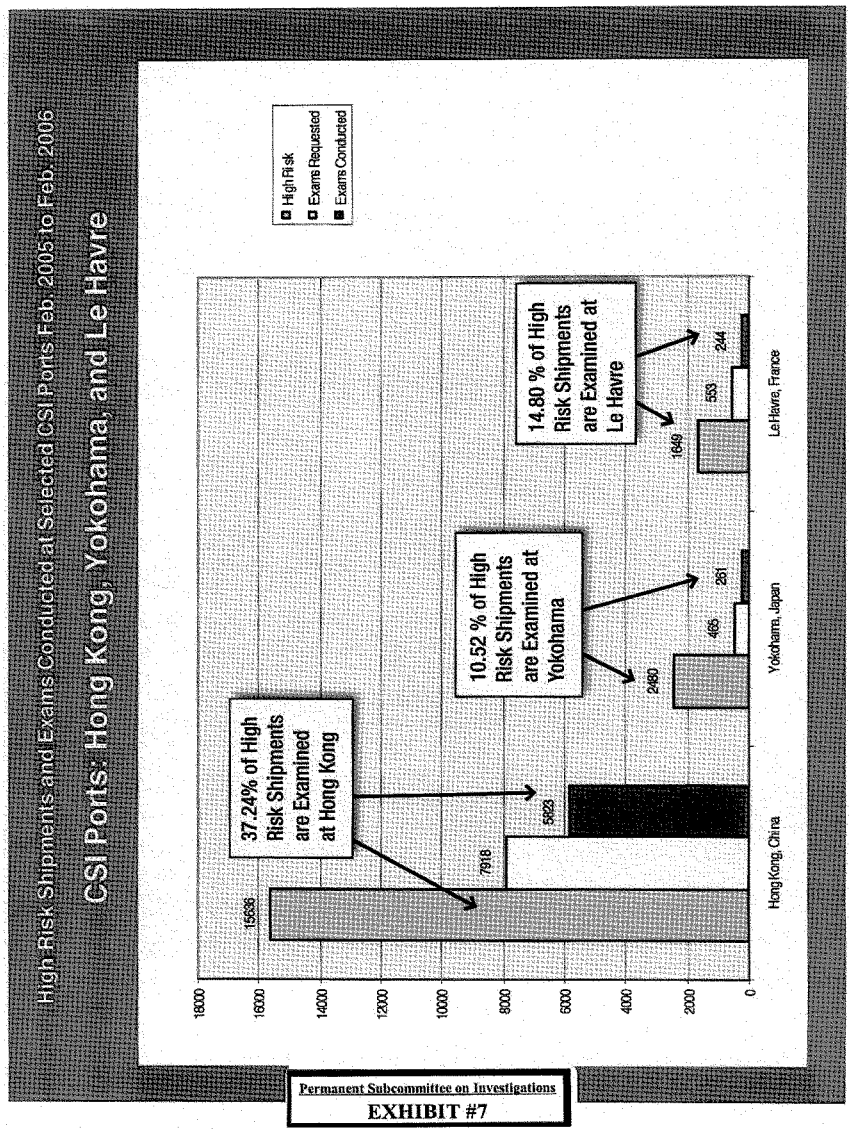
GAO Contact and Staff Acknowledgments

GAO Contact Gregory D. Kutz (202) 512-7455

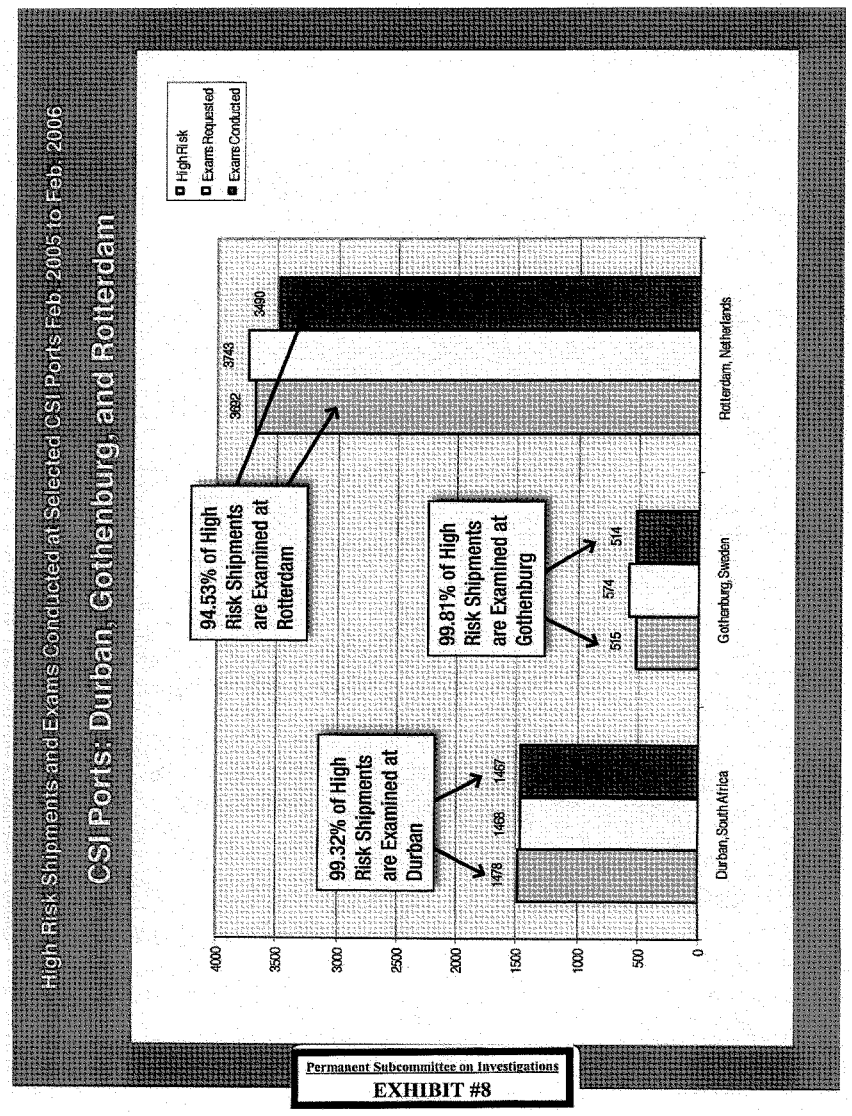
Acknowledgments In addition to the individual named above, Andrew O'Connell, Richard Egan, John Cooney, Paul Desaulniers, Christine Hodakievic, George Ogilvie, Rich Hung, Jim Shafer, Stockton Butler, Kord Basnight, and Renee McElveen made key contributions to this report.

(192203)


High Risk Shipments and Exams for all CSI Ports Feb.2005 - Feb.2006
Total Volume
High Risk
Exams Requested
Exams Conducted
10000000
9000000
8000000
7000000
6000000
5000000
4000000
3000000
2000000
1000000
0
9264513
130912
58945
48747
1
37.24% of High Risk Shipments are Examined at All CSI Ports
Permanent Subcommittee on Investigations
EXHIBIT #6



Permanent Subcommittee on Investigations
EXHIBIT #7



Permanent Subcommittee on Investigations
EXHIBIT #8

CONGRESSIONAL BUDGET OFFICE
U.S. Congress
Washington, DC 20515

March 29, 2006

Honorable Norm Coleman
Chairman
Permanent Subcommittee on Investigations
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

In response to your request about the economic effect of disruptions to the flow of container shipments at major U.S. ports, the Congressional Budget Office is issuing the attached analysis, *The Economic Costs of Disruptions in Container Shipments*.

The details of CBO's response are contained in the attachment. If you have any questions or need further information, please feel free to call me, at (202) 226-2700, or Joseph Kile, the staff contact for this work, at (202) 226-2940.

Sincerely,

Donald B. Marron

Donald B. Marron
Acting Director

Attachment

cc: Honorable Carl Levin
Ranking Minority Member

Honorable Susan M. Collins
Chair
Committee on Homeland Security and Governmental Affairs

Honorable Joseph I. Lieberman
Ranking Member

The Economic Costs of Disruptions in Container Shipments

March 29, 2006

The Congress of the United States ■ Congressional Budget Office

Notes

This report was written by Bruce Arnold, Craig Cammarata, Dick Farmer, Kim Kowalewski, Fatimot Ladipo, Mark Lasky, and David Moore of the Congressional Budget Office (CBO), under the supervision of Robert Dennis and Joseph Kile. Technical advice and helpful comments on an earlier draft were provided by Peter Hall of the University of Waterloo, William D. Nordhaus of Yale University, and Nouriel Roubini of New York University. (The assistance of external reviewers implies no responsibility for the final product, which rests solely with CBO.) In keeping with CBO's mandate to provide objective, impartial analysis, this report makes no recommendations.

Unless otherwise indicated, all estimates of the economic costs of a port closure are in 2006 dollars.

Numbers in the text, tables, and figures may not add up to totals because of rounding.

Contents

Tables

Figures

Boxes

Introduction and Summary

The security threat posed by the nearly 24 million shipping containers that arrive each year at U.S. ports is a major concern for policymakers.[1] That concern is partly motivated by the loss of life and damage to property that could occur from a terrorist attack using incoming containers. Another source of concern is the potential loss to the economy if one or more major U.S. ports were shut down for any length of time.

Roughly one-quarter of the United States' imports and one-sixth of its exports—or about $423 billion and $139 billion worth of goods, respectively, in 2004—arrive or depart on container ships. Containerized imports include both finished goods and intermediate inputs, some of which are critical to maintaining U.S. manufacturers' "just-in-time" supply chains. Such supply chains have been widely adopted, but they can leave manufacturers vulnerable to disruption if a necessary part does not reach an assembly plant in time. The lack of key parts could reduce output, employment, and income for individual companies by amounts larger than the value of the delayed part—and in areas and businesses far removed from the port where a disruption occurred. Although concerns about disruptions in the flow of container traffic focus on terrorist attacks, similar economic losses could result from extreme weather or labor disputes that affected port operations or from disruptions elsewhere in the supply chain.

At the request of the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs, the Congressional Budget Office (CBO) analyzed the national economic costs of disruptions in container traffic, regardless of their cause. This report summarizes the structure and economics of the U.S. port industry and container traffic, estimates the economic cost of various disruptions in that traffic, and discusses how such disruptions might affect the economy.

As requested by the Subcommittee, the analysis focuses on two specific disruption scenarios:

- An unexpected one-week halt to all container traffic through the ports of Los Angeles and Long Beach, California, the country's two largest ports for such shipments; and
- An unexpected three-year halt to all container traffic through those two ports as well as an initial precautionary one-week stoppage of container shipments at all U.S. ports.

1. That estimate of annual incoming container traffic is measured in 20-foot equivalent units, or TEUs (the amount of cargo that fits in a 20' x 8' x 8' container), and comes from U.S. Maritime Administration, *Containership Market Indicators* (August 2005), available at www.marad.dot.gov/MARAD_statistics/2005%20STATISTICS/Container%20Market%20Indicators.pdf.

CBO's analysis of those scenarios provides rough estimates of the costs to the U.S. economy of disruptions in container traffic. Although in 2004 approximately $500 million worth of containerized imports flowed into the ports of Los Angeles and Long Beach each day, the loss in production (gross domestic product, or GDP) from a one-week shutdown of those ports would probably be less—between $65 million and $150 million per day.

Daily costs would be at least that large in the case of a three-year closure of those ports and an initial one-week stoppage of container movement at all U.S. ports. Simulations commissioned by CBO suggest that the three-year shutdown would reduce real (inflation-adjusted) GDP by between 0.35 percent and 0.55 percent, or $45 billion to $70 billion, per year.[2] That reduction translates into daily costs ranging from $125 million to $200 million.

Spending by consumers and businesses would fall substantially more than that during the shutdown. The reason is that consumers and businesses would spend less on both imported goods and domestically produced goods, but the decline in real GDP reflects only reductions in domestic production. Inflation, as measured by consumer prices, would be higher in the first year (by about 2 percentage points) than it would have been otherwise, little changed in the second year, and lower thereafter, eventually bringing the level of consumer prices back to where it would have been without the disruption. Employment would be an average of about 1 million jobs lower during the three years of the shutdown, according to the simulations.

The estimates for a short closure of the Los Angeles and Long Beach ports would also apply to a shutdown of one or more foreign ports if comparable flows of trade were affected. Of particular interest is the trade flowing through the word's largest ports, which are predominantly in Asia. However, Asian exporters seeking to move goods to the United States would most likely have more alternatives for rerouting shipments than would U.S. importers seeking to receive goods through West Coast ports. Thus, a disruption in port activity of a similar scale in Asia would have a smaller effect on the U.S. economy.

The estimates presented in this report are for the U.S. economy as a whole. They do not focus on distributional effects. When shipments are diverted from one port to another—as would occur if the Los Angeles and Long Beach ports closed for a long period—income and jobs would shift with them. From the perspective of the national economy, gains elsewhere would offset some of the losses in the directly affected area. But that economic activity would not produce income for the workers employed by, or returns on the capital invested in, the ports of Los Angeles and Long Beach. Similarly, firms—particularly those with the lean supply chains characteristic of just-in-time production—would be forced to reduce their output in some scenarios. How-

2. As discussed below, the simulations were conducted by Inforum (a nonprofit research organization affiliated with the University of Maryland) using its LIFT economic model, with assumptions supplied by CBO. For more details about the estimating methods, see Appendix A.

ever, other firms that had different supply chains or that produced competing goods or entirely different products might increase their output. The cost to the national economy of a disruption would reflect the losses of some firms and the gains of others.

These estimates are not based on an analysis of specific bottlenecks that could arise because of a manufacturer's reliance on just-in-time inventories. CBO lacks information about which companies and industries control their inventories in that way and about whether they do so for goods that would be shipped in containers through Los Angeles and Long Beach. However, there are reasons to suspect that bottlenecks due to just-in-time inventories would not have a large impact on these estimates. The manufacturers that use such inventory-control methods are likely to be the ones with the most sophisticated logistics systems, and thus they may be in the best position to find alternate supply routes on short notice. In addition, most of the containerized imports that arrive at the Los Angeles and Long Beach ports appear to be finished goods, not intermediate inputs. Thus, the main loss from a shutdown would be a loss of final sales, which CBO's analytic methods measure adequately.

U.S. Ports and Merchandise Trade

Ports are a gateway for imports and exports of both finished and intermediate goods. In 2004, nearly $1.5 trillion worth of goods were imported to the United States, and $0.8 trillion of U.S. goods were exported to other countries. Almost half of the imported goods arrived by sea (see Figure 1). The United States is home to about 360 commercial ports, but just 20 handle more than 80 percent (by total value) of goods imports and exports. Moreover, the largest three ports—Los Angeles, New York, and Long Beach—handled about 40 percent of the U.S. imports that arrived by water in 2004 (see Table 1).

Container Shipping

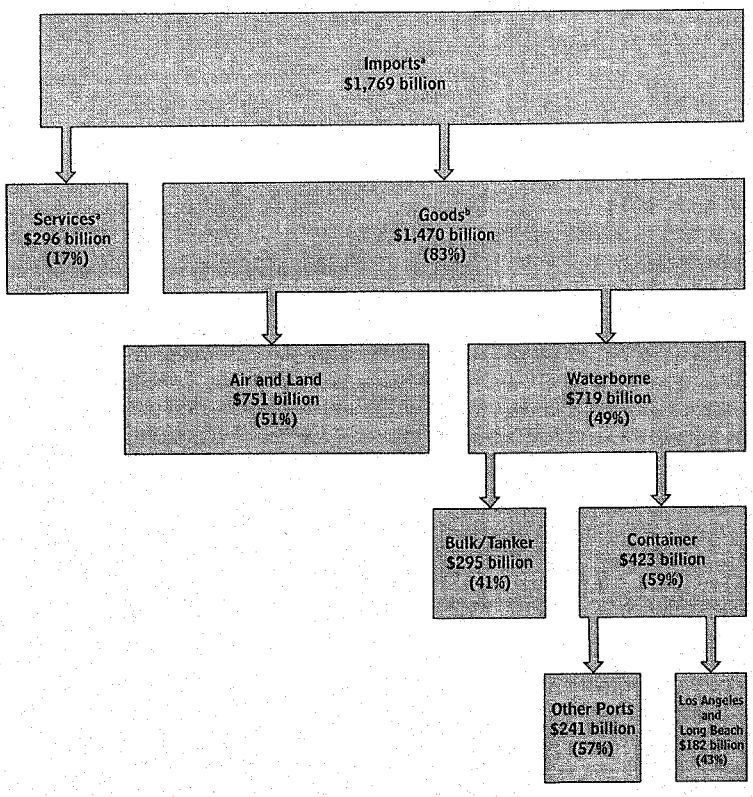
A growing share of waterborne imports travel by container ship. Such ships come in several sizes; the largest that now call at U.S. ports carry more than 8,000 containers.[3] Containers allow for standardized handling and shipping practices and integration with rail and truck distribution networks. Those factors give container shipping a cost advantage for many goods. Container traffic has been growing steadily in the past decade, reflecting growth in international trade and changes in the economics of transport by sea relative to other modes.

Container ships tend to carry items that are relatively high in value per unit. In 2004, containerized imports arriving at U.S. ports were valued at a total of $423 billion, or almost one-quarter of the value of all U.S. imports. Containerized exports from U.S. ports that year had a total value of about $139 billion.

3. Yvonne Smith, "Executive Overview: Pacific Maritime," *World Trade* (February 25, 2006), available at www.worldtrademag.com/CDA/Articles/Feature_Article/2006d39c1fd99010VgnVCM100000f932a8c0.

Figure 1.

U.S. Containerized Imports in Perspective, 2004



Source: Congressional Budget Office based on data from the Bureau of the Census, Foreign Trade Division; the U.S. Maritime Administration; and Bureau of the Census, *U.S. International Trade in Goods and Services: January 2006* (March 9, 2006), Exhibits 1 and 5.

Note: All data are customs values.

a. Total imports and services are reported on a balance-of-payments basis.

b. Goods imports are reported on a Census basis. For comparison, goods imports in 2004 were $1,473 billion on a balance-of-payments basis.

Table 1.

Top 20 U.S. Ports for All Waterborne Imports and Exports, by Value, 2004

(Billions of dollars)

Port	Value	Port	Value
Waterborne Imports		Waterborne Exports	
Los Angeles, California	130.7	Houston, Texas	29.1
New York, New York	90.2	New York, New York	23.1
Long Beach, California	74.8	Los Angeles, California	17.8
Houston, Texas	36.8	Long Beach, California	17.3
Charleston, South Carolina	30.8	Charleston, South Carolina	15.3
Baltimore, Maryland	24.4	Norfolk, Virginia	12.0
Tacoma, Washington	22.5	Savannah, Georgia	9.7
Seattle, Washington	22.4	New Orleans, Louisiana	9.6
Norfolk, Virginia	21.2	Oakland, California	8.7
Oakland, California	18.3	Miami, Florida	7.7
Philadelphia, Pennsylvania	16.6	Port of South Louisiana	7.6
Savannah, Georgia	16.3	Baltimore, Maryland	6.9
Morgan City, Louisiana	14.1	Seattle, Washington	6.8
New Orleans, Louisiana	12.6	Tacoma, Washington	5.3
Beaumont, Texas	12.0	Port Everglades, Florida	4.8
Miami, Florida	10.7	Jacksonville, Florida	4.5
Corpus Christi, Texas	9.9	Portland, Oregon	3.1
Jacksonville, Florida	9.2	Anchorage, Alaska	2.4
Portland, Oregon	9.1	Corpus Christi, Texas	2.0
Wilmington, Delaware	7.7	Tampa, Florida	1.7
Total, Top 20 Ports	**590.3**	**Total, Top 20 Ports**	**195.5**
All U.S. Ports	**718.7**	**All U.S. Ports**	**229.9**

Source: Congressional Budget Office based on information from the U.S. Maritime Administration.

Not all U.S. ports are equipped to accommodate container shipping. Different ports have very different unloading capabilities and handle different types of vessels. Ports on the Gulf Coast handle a large share of tankers and dry bulk cargo, whereas those on the East and West Coasts handle a large percentage of container traffic and vehicle shipping. Because of those differences, the economic consequences of closures at particular ports can vary greatly.

West Coast Ports

The West Coast is home to three of the top five U.S. ports for receiving containerized goods (ranked by value) and to the second- and third-largest ports for exporting them (see Table 2). The United States exports far fewer containers than it imports.

Table 2.

Top 20 U.S. Ports for Containerized Imports and Exports, by Value, 2004

(Billions of dollars)

Port	Value	Port	Value
Containerized Imports		**Containerized Exports**	
Los Angeles, California	118.7	New York, New York	19.5
Long Beach, California	63.5	Los Angeles, California	16.0
New York, New York	61.4	Long Beach, California	15.7
Charleston, South Carolina	24.2	Houston, Texas	12.1
Seattle, Washington	21.0	Charleston, South Carolina	10.9
Norfolk, Virginia	20.1	Norfolk, Virginia	10.4
Tacoma, Washington	19.6	Oakland, California	8.0
Oakland, California	17.7	Savannah, Georgia	7.8
Savannah, Georgia	12.8	Miami, Florida	5.9
Houston, Texas	11.3	Seattle, Washington	5.6
Miami, Florida	10.0	Tacoma, Washington	3.8
Baltimore, Maryland	9.5	Port Everglades, Florida	3.6
Port Everglades, Florida	4.9	New Orleans, Louisiana	3.2
New Orleans, Louisiana	3.2	Baltimore, Maryland	2.8
Philadelphia, Pennsylvania	3.1	Jacksonville, Florida	1.6
San Juan, Puerto Rico	2.5	Portland, Oregon	1.3
Gulfport, Mississippi	2.2	Gulfport, Mississippi	1.1
Boston, Massachusetts	2.0	Philadelphia, Pennsylvania	1.1
Portland, Oregon	1.8	San Juan, Puerto Rico	1.1
Chester, Pennsylvania	1.7	Chester, Pennsylvania	0.8
Total, Top 20 Ports	**411.3**	**Total, Top 20 Ports**	**132.3**
All U.S. Ports	**423.4**	**All U.S. Ports**	**139.3**

Source: Congressional Budget Office based on information from the U.S. Maritime Administration.

The ports of Los Angeles and Long Beach, both situated on California's San Pedro Bay, are the nation's busiest ports for containerized imports. In 2004, they handled 43 percent of such imports (by value), or more than $180 billion worth (see Table 3). Those imports accounted for just over 12 percent of the value of all goods imported into the United States. The value of containerized exports from Los Angeles and Long Beach was considerably smaller, just over $30 billion, and accounted for a smaller share of total U.S. containerized exports, about 23 percent (see Table 4). The relative importance of container traffic at Los Angeles and Long Beach is even greater on the West Coast, where those two ports accounted for two-thirds of the value of total container shipments in 2004 (see Figure 2). According to the Department of Transporta-

Table 3.

Top 20 Containerized Imports, by Value, 2004

HS#	Category of Import	Los Angeles and Long Beach Ports		All U.S. Ports	
		Value (Billions of dollars)	Percentage of Total Containerized Imports of That Commodity	Value (Billions of dollars)	Percentage of Total Containerized Imports Nationwide
84	Machinery, Boilers, Reactors, Parts	38.0	50.7	74.8	17.7
85	Electric Machinery, Sound and Television Equipment, Parts	31.7	64.1	49.4	11.7
87	Vehicles and Parts, Except Railway or Tramway	12.1	39.3	30.8	7.3
61	Apparel Articles and Accessories, Knit or Crochet	9.0	39.1	23.1	5.5
62	Apparel Articles and Accessories, Not Knit or Crochet	9.9	44.0	22.5	5.3
94	Furniture, Bedding, Lamps, Etc.	9.3	48.4	19.3	4.6
95	Toys, Games, and Sports Equipment and Parts	9.4	55.8	16.9	4.0
64	Footwear	7.8	56.0	13.9	3.3
39	Plastics and Articles Thereof	5.2	41.1	12.7	3.0
73	Articles of Iron or Steel	4.4	44.6	9.8	2.3
22	Beverages, Spirits, and Vinegar	0.9	10.0	8.7	2.1
40	Rubber and Articles Thereof	3.5	43.8	7.9	1.9
90	Optic, Photographic, and Medical Instruments	3.6	47.0	7.7	1.8
29	Organic Chemicals	1.3	19.1	6.6	1.6
63	Textile Articles, Needlecraft, Worn Textile Articles	2.6	40.6	6.4	1.5
44	Wood and Wood Articles	1.6	26.2	6.2	1.5
42	Leather Articles, Saddlery, Handbags	3.8	63.7	5.9	1.4
03	Fish, Crustaceans	2.1	39.6	5.3	1.3
30	Pharmaceutical Products	0.1	2.8	4.7	1.1
48	Paper and Paperboard	1.4	32.5	4.5	1.1
	Total, Top 20 Containerized Imports	**157.7**	**46.8**	**337.1**	**79.6**
All Containerized Imports		**182.3**	**43.0**	**423.4**	**100.0**

Source: Congressional Budget Office based on information from the U.S. Maritime Administration.

Note: HS = Harmonized Commodity Description and Coding System.

Table 4.

Top 20 Containerized Exports, by Value, 2004

HS#	Category of Export	Los Angeles and Long Beach Ports		All U.S. Ports	
		Value (Billions of dollars)	Percentage of Total Containerized Exports of That Commodity	Value (Billions of dollars)	Percentage of Total Containerized Exports Nationwide
84	Machinery, Boilers, Reactors, Parts	4.9	22.3	21.8	15.7
39	Plastics and Articles Thereof	3.5	27.6	12.5	9.0
87	Vehicles and Parts, Except Railway or Tramway	1.9	22.6	8.3	6.0
85	Electric Machinery, Sound and Television Equipment, Parts	2.3	30.1	7.6	5.5
29	Organic Chemicals	1.9	24.4	7.6	5.5
52	Cotton, Including Yarn and Fabric	1.9	41.1	4.7	3.3
38	Miscellaneous Chemical Products	1.0	23.1	4.4	3.2
48	Paper and Paperboard	0.4	10.1	3.8	2.7
90	Optic, Photographic, and Medical Instruments	0.9	24.8	3.7	2.7
28	Inorganic Chemicals	0.5	16.6	3.2	2.3
08	Edible Fruit and Nuts	0.7	27.2	2.7	1.9
40	Rubber and Articles Thereof	0.6	22.3	2.5	1.8
24	Tobacco and Tobacco Substitutes	0.4	14.4	2.5	1.8
47	Wood Pulp, Recovered Paper Waste and Scrap	0.4	15.6	2.3	1.7
33	Essential Oils, Perfumes, Cosmetics	0.6	24.8	2.3	1.6
02	Meat	0.2	9.9	2.1	1.5
44	Wood and Wood Articles	0.2	7.5	2.1	1.5
32	Tanning Extracts, Dyes, Paint, Ink, Etc.	0.4	21.7	2.0	1.4
41	Raw Hides, Skins, and Leather	0.7	40.1	1.8	1.3
72	Iron and Steel	0.5	26.4	1.8	1.3
	Total, Top 20 Containerized Exports	**23.7**	**23.8**	**99.6**	**71.5**
All Containerized Exports		**31.7**	**22.7**	**139.3**	**100.0**

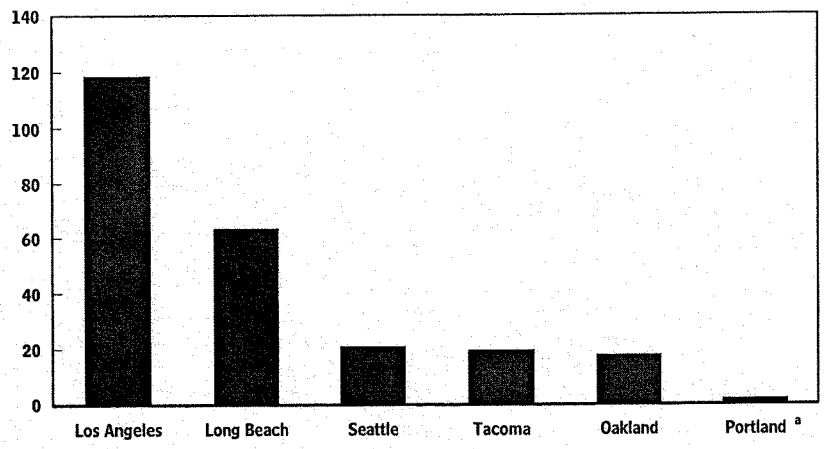
Source: Congressional Budget Office based on information from the U.S. Maritime Administration.

Note: HS = Harmonized Commodity Description and Coding System.

Figure 2.

Value of Containerized Imports at the Six Largest West Coast Ports, 2004

(Billions of dollars)



Source: Congressional Budget Office based on information from the U.S. Maritime Administration.

a. Less than $2 billion.

tion, container trade at those ports nearly doubled between 1994 and 2004, about the same as growth in containerized cargo overall.[4]

Imports into Los Angeles and Long Beach are predominantly finished goods rather than intermediate ones. The simulations discussed below suggest that almost two-thirds of the containerized goods received at those ports are likely to be finished goods.

Capacity Constraints

The constraints on container traffic are complex, depending on the capacity at several points in the supply chain. In general, containerized cargo in the United States moves from place to place through a network—called intermodal shipping—that links vessels, port terminals, and trucks and trains. To receive container ships, a port must have a deep enough channel to accommodate large vessels and enough berths where those ships can tie up. In addition, to manage the containers, a port must have:

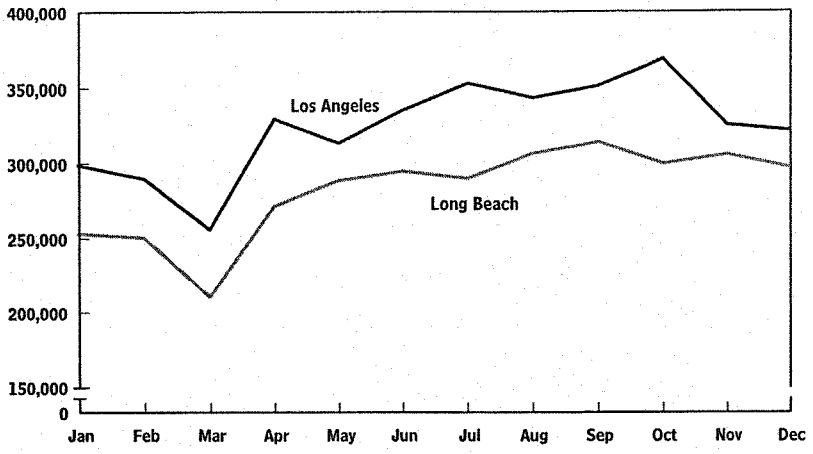
- Special equipment for loading and unloading containers to and from ships,

4. Department of Transportation, *Freight Facts and Figures 2005* (November 2005), Figure 2-8 (available at www.ops.fhwa.dot.gov/freight/freight_analysis/nat_freight_stats/docs/05factsfigures/fig2_8.htm).

Figure 3.

Monthly Containerized Imports at Los Angeles and Long Beach Ports, 2005

(In 20-foot equivalent units)



Source: Congressional Budget Office based on information from the Port of Los Angeles and the Port of Long Beach.

Note: Marine containers come in various sizes. To allow for consistency in comparisons, those sizes are commonly presented in terms of a standard 20-foot container. For example, one 40-foot container would be counted as two 20-foot equivalent units.

- On-dock storage space and equipment for moving containers to local terminals (or to storage and distribution centers farther inland), and
- Intermodal connections for loading containers on trucks or rail cars.

Assuming that container ships can enter a port and that enough skilled labor exists to fully use cranes for loading and unloading, a key bottleneck on traffic often becomes dock space. As the stacks of containers on the dock grow, the process of sorting among them and of locating and moving individual containers to specific terminals or intermodal connections can quickly bog down. Moreover, when containers make it to the point of leaving the port, sufficient truck and rail capacity must be available to carry them away. Constraints on rail capacity, for example, contributed to a slowdown in the distribution of imports in late 2004.[5]

On the West Coast, options for diverting traffic from one port to another are limited by the existence of few natural harbors (mainly San Pedro Bay, San Francisco Bay, and

5. Congressional Budget Office, *Freight Rail Transportation: A Review of the 2004 Experience* (May 2005), pp. 5-7.

Puget Sound). In addition, shippers' ability to divert container traffic is likely to vary depending on the time of year. Seasonal peaks in traffic into Los Angeles and Long Beach, for example, occur in the late summer and fall; traffic is lighter in the winter and early spring (see Figure 3).

Two Disruption Scenarios and Estimates of Their Cost to the Economy

At the direction of the Subcommittee, CBO considered two alternative scenarios involving disruptions at U.S. ports:

- A brief unexpected disruption of container traffic at the ports of Los Angeles and Long Beach. CBO assumed that the initial blockage would last one week but that the backlog of shipments would require at least one month to clear through other West Coast ports, air deliveries, and a reopened Los Angeles and Long Beach.

- A lengthy unexpected disruption of container traffic at Los Angeles and Long Beach coupled with a brief precautionary halt to container traffic at all U.S. ports. CBO assumed that the lengthy disruption would entail the total closure of Los Angeles and Long Beach for three years, after which those ports would fully reopen for business. During the closure, a share of those ports' former traffic would be diverted to other ports. The brief disruption for all other U.S. ports was assumed to last only one week, but the backlog of shipments, combined with the diversion of some traffic from Southern California, would require at least three months to clear.

The economic cost of a port closure would depend on its duration and on how shippers, producers, and consumers adapted to the shutdown. For a brief disruption, the cost would depend greatly on how the backlog of ships waiting to enter ports was resolved. In 2002, when a labor dispute closed major West Coast ports for 11 days, almost all ships were able to land within the next month, so the net impact on annual trade was minimal.

A disruption lasting more than a few days would have higher daily costs, because the measures taken by shippers and producers would become less effective the longer that traffic was disrupted. Inventories would be depleted, and cost-effective options to shift cargo to air would be exhausted. As months went by, however, shippers, producers, and consumers would adapt in ways that would reduce the daily economic cost of a disruption. The capacity of alternative ports would be expanded. Supply chains would be reconfigured, though perhaps at a higher cost than before the disruption. Producers might turn to domestic sources of supply, and consumers might choose to purchase a different mix of goods. Those types of adjustments—and the resilience of the economy that they imply—have been evident in the past in response to both natural disasters and the terrorist attacks of September 11, 2001 (see Box 1).

Box 1.

The Economic Costs of Previous U.S. Disasters

The economic damage that resulted from previous disasters offers some insight into the harm that could occur from a disruption of port traffic. In the case of the September 11 terrorist attacks and recent hurricanes, widespread losses of life, property, and jobs and disruptions of transportation networks caused significant economic damage to specific areas as well as to individuals and businesses. Those disasters also harmed the U.S. economy, but the total economic impact was less than had initially been feared.

Analysis of past disasters suggests that they have not had a large sustained effect on the national economy. For example, an examination of some disasters in the 1990s (the Northridge earthquake and Hurricanes Andrew and Floyd) concluded that gross state product recovered fully within a single quarter.[1]

September 11 Terrorist Attacks

According to a report by the Federal Reserve Bank of New York, the terrorist attacks of September 11, 2001, cost New York City an estimated $33 billion to $36 billion. That total comprises $7.8 billion in lost earnings of deceased workers, $3.6 billion to $6.4 billion in reduced wage and salary income of other workers, and $21.6 billion in costs for property damage and cleanup of the site.[2]

Those losses caused productivity to decline for several months locally and consumer confidence to drop nationwide. Air travel and consumer spending also fell. According to *Blue Chip Economic Indicators*, the outlook for the growth of real (inflation-adjusted) gross domestic product (GDP) in 2002 dropped sharply: from 2.7 percent just before the attacks to 1.0 percent the following January.[3] Real GDP actually grew by 1.6 percent in 2002, exceeding that expectation.

1. Edward E. Leamer and Christopher Thornberg, *The Economic Impact of the Terrorist Attack on the World Trade Center Will Be Minor* (Los Angeles: UCLA Anderson Forecast, September 13, 2001), p. 2.
2. Jason Bram, James Orr, and Carol Rapaport, "Measuring the Effects of the September 11 Attack on New York City," *Economic Policy Review*, Federal Reserve Bank of New York, vol. 8, no. 2 (November 2002).
3. Aspen Publishers, Inc., *Blue Chip Economic Indicators*, vol. 27, no. 1 (January 10, 2002) p. 3, and *Blue Chip Economic Indicators*, vol. 26, no. 9 (September 10, 2001), p. 2.

Box 1.

Continued

Hurricanes Katrina and Rita

Hurricanes Katrina and Rita had an immediate effect on the economic activity of the Gulf Coast region as well as on the nation. Besides costing lives and damaging property, the hurricanes reduced energy production, which immediately drove up energy prices nationwide. Initial estimates of the total loss of physical capital attributable to those storms ranged from $70 billion to $130 billion.[4]

The effects of Hurricanes Katrina and Rita may have slowed the growth of real GDP during the second half of 2005 by roughly 0.5 percentage points.[5] The Congressional Budget Office estimates that GDP growth is likely to be boosted by a similar amount in the first half of 2006 as energy production comes back online and efforts to rebuild local communities stimulate the economy.

GDP Versus Standard of Living

Gross domestic product is a measure of economic output, not standards of living. Disasters often produce little or no long-term change in GDP, although they may drastically reduce the standard of living of people affected by them. Increased economic activity after a disaster helps to restore previous living standards. Rebuilding boosts GDP but by itself may not leave people as well off as they were before the disaster.

4. Statement of Douglas Holtz-Eakin, Director, Congressional Budget Office, "Macroeconomic and Budgetary Effects of Hurricanes Katrina and Rita," before the House Committee on the Budget, October 6, 2005, p. 3.

5. Congressional Budget Office, *The Budget and Economic Outlook: Fiscal Years 2007 to 2016* (January 2006), Box 2-1.

The estimates provided in this report are for a disruption of container trade caused by a shutdown of U.S. ports. The economic cost would be much the same from a shutdown of one or more foreign ports if the closure affected comparable trade flows. In the case of trans-Pacific trade, however, businesses that ship goods from Asia to the United States have more alternatives available to them than do the recipients of those goods in the United States. Thus, comparable disruptions of ports in Asia would have smaller effects on the United States. (Appendix B discusses a disruption of container shipments from the port of Hong Kong and options to reroute trade in that region.)

CBO's analysis focuses on the impact of lost trade opportunities. As such, it does not estimate the cost of other losses that might occur at the same time, such as the value of lives that could be lost in a terrorist attack on a port, the cost of replacing lost capital and equipment, or the additional costs of security changes that might be made in response to an attack.

A One-Week Shutdown of the Ports of Los Angeles and Long Beach

Previous studies of port closures and a simulation of the Subcommittee's short-term scenario shed light on the economic cost of the loss of container trade that would result from a weeklong port shutdown. Although about $500 million worth of containerized imports flowed daily into the ports of Los Angeles and Long Beach in 2004, closure of those ports for one week could cost the U.S. economy somewhere in the range of $65 million to $150 million per day. The lower end of that range comes from an estimate of how much shippers are willing to pay to avoid delays and from an analysis by the economic forecasting firm DRI-WEFA (now Global Insight) of the cost of a hypothetical shutdown of all West Coast ports. The high end of the range comes from a simulation specified by CBO and estimated by Inforum using its LIFT (Long-Term Interindustry Forecasting Tool) model.

The LIFT Simulation. CBO contracted with Inforum, a nonprofit economic consulting group affiliated with the University of Maryland, to simulate the Subcommittee's scenarios using Inforum's LIFT model of the national economy and assumptions supplied by CBO about the disruptions. LIFT can examine the macroeconomic effects over time of industry-specific disruptions, such as a loss of imports or exports. The assumptions supplied by CBO specified reductions in U.S. imports of certain goods, consistent with the amounts that had been arriving at Los Angeles and Long Beach. Those amounts were net of assumed diversions of some containerized imports to other ports (including ones in Canada and Mexico) and to other modes of transportation (including some transshipment to bulk cargo and air freight). The LIFT model and the simulation assumptions are described in greater detail in Appendix A.

The results of the LIFT model simulation indicate that a one-week shutdown of container traffic through Los Angeles and Long Beach would have a small and temporary impact on the national economy. For an average week, it would reduce GDP by $150 million per day, at most. That reduction would be temporary; once the shutdown was resolved and the delayed imports arrived and were processed, GDP would return to where it would otherwise have been.

If businesses cut employment in line with their loss of output, job losses for the week could be quite large, because the port shutdown would affect low-wage industries with relatively high numbers of employees more than high-wage industries with fewer employees. However, in a brief shutdown, many businesses would probably continue to pay idled workers until conditions returned to normal.

Those estimates most likely overstate the actual reductions in production and employment because they do not account for the increase in imports that would occur in the month after the shutdown as the backlog was cleared. Moreover, the simulation assumes that businesses do not reduce their inventories to maintain production as much as they probably would for a shutdown that lasted only a week.

Estimates of the Economic Cost of the 2002 Port Closure. Major West Coast ports were closed by a labor dispute from September 29 to October 9, 2002. A number of studies have produced estimates (both prospectively and after the fact) of the economic costs of such a shutdown.

A DRI-WEFA study of a closure of West Coast ports provides the basis for an estimate of roughly $75 million per day in costs to the economy from a seven-day shutdown of container traffic through the ports of Los Angeles and Long Beach.[6] That study's approach to estimating the cost of a disruption is in many ways similar to that of the LIFT simulations. To evaluate the Subcommittee's scenario for a one-week disruption, CBO adjusted the DRI-WEFA estimate to account for growth in the volume and value of container traffic since 2002 and the characteristics of the scenario. The DRI-WEFA estimate was for a shutdown in July, an average month for container traffic (see Figure 3). The cost would be larger in an above-average (fall) month and lower in a below-average (winter) month. The scenario considered in this analysis envisions an unanticipated shutdown, but DRI-WEFA assumed that shippers would anticipate a closure and take actions to reduce its costs. For that reason, the adjusted DRI-WEFA estimate may understate the cost of the short-term disruption evaluated in this analysis.

Another study estimated a cost of $1.9 billion per day for a 10-day closure of West Coast ports in 2000. However, in CBO's view, that estimate overstates the likely cost of the 2002 shutdown because of the limited nature of the impact-study approach used to produce the estimate (see Box 2 for more details).

Estimates Based on Shippers' Willingness to Pay to Avoid Delays. A 2001 study analyzed U.S. import data on a product-by-product basis for the mode of transport that shippers used (sea or air), the required transit time for a product by sea (air transit time was assumed to be one day), and the extra expense required for air shipment versus slower ocean shipment.[7] On the basis of that analysis, the study estimated that each day saved in shipping was worth, to an importer, 0.8 percent of the value of the goods being shipped. The converse is that each day of delay resulting from a port closure would cost the importer 0.8 percent of the value of the goods being shipped.

---

6. DRI-WEFA, *The National Economic Impact of a West Coast Port Shutdown* (prepared for the Department of Labor, Office of the Assistant Secretary for Policy, May 29, 2002).

7. David Hummels, *Time as a Trade Barrier* (working paper, Purdue University, July 2001), available at www.mgmt.purdue.edu/faculty/hummelsd/research/time3b.pdf.

Box 2.

Differences Between an Impact Study and an Interindustry Study

Impact studies, such as those performed to assess the impact of port shutdowns or slowdowns, tend to estimate much larger economic effects from a port closure than do studies that use an interindustry approach. As one critic of them notes, port impact studies "typically assume fixed technology, industrial structure, and demand," whereas interindustry studies do not.[1] In addition, impact studies may include losses in business revenues that do not reflect net losses to U.S. income or output.

A widely cited 2001 impact study concluded that a 10-day shutdown of West Coast ports would cost the economy $1.9 billion per day.[2] The ports and related transportation links would absorb about 4 percent of that total cost, and importers, exporters, and supporting industries would absorb the rest. However, the estimate of the economic impact to importers includes the amount they pay to foreign suppliers for those imports, which would be a loss to the foreign suppliers but not a net loss to U.S. businesses. The study assumes that the ratio of direct and indirect business revenues from containerized cargo activity at West Coast ports to direct and indirect wages and salaries from that activity is 8.2. In 2000, the ratio of gross domestic product (GDP)—a better measure of domestic activity than business revenues are—to wages and salaries was 2.0. Scaling the study's estimate of $1.9 billion per day down by 2.0/8.2 would reduce the economic impact of such a shutdown to $470 million per day.

Even that estimate assumes that the economy adjusts much less in response to an adverse supply shock than an interindustry model such as LIFT assumes. For example, consider the case of electric lighting and wiring equipment. Such equipment is an important input to construction, accounting for 1.6 percent of the value of new construction in 1998. The roughly $25 million of electric lighting and wiring equipment imported daily through the ports of Los Angeles and Long Beach accounts for about 10 percent of U.S. demand for those items. If technology, industrial structure, and demand were fixed—as in an impact study—the loss of those imports could have a severe impact on construction.

---

1. Peter V. Hall, "We'd Have to Sink Ships': Impact Studies and the 2002 West Coast Port Lockout," *Economic Development Quarterly*, vol. 18, no. 4 (November 2004), pp. 354-367.

2. Martin Associates, *An Assessment of the Impact of West Coast Container Operations and the Potential Impacts of an Interruption of Port Operations, 2000* (Lancaster, Pa.: Martin Associates, October 23, 2001), prepared for the Pacific Maritime Association.

Box 2.

Continued

According to the interindustry study conducted by the Congressional Budget Office, however, the economy would adjust to such a loss in several ways:

- A substantial portion of the imports normally entering the United States through the closed ports would simply enter the country elsewhere. Such diversions of traffic would reduce the decline in imports of electric lighting and wiring equipment in a one-week shutdown from about $25 million per day to $16 million.

- U.S. producers of such equipment would make up for some of the shortfall. Results from the LIFT model—in which producers respond to the higher prices that domestic goods would command with less competition from imports—suggest that manufacturers would increase production by $8 million per day (compared with what they would otherwise produce) in a one-week port shutdown.

- Sellers and users of electric lighting and wiring equipment could draw down domestic inventories of such items. That might make available another $2 million per day in a weeklong shutdown. (That estimate probably understates the ability of businesses to draw down inventories during a one-week closure.)

With those factors taken into account, the U.S. supply of lighting and wiring equipment would decline by just $6 million per day in a one-week port shutdown—much less than the $25 million normally imported through Los Angeles and Long Beach. Failing to account for those adjustment factors would increase losses to the construction industry by a factor of more than four.

Two other factors could trim that loss further. First, the percentage of imports diverted from the Los Angeles and Long Beach ports would most likely be greater for important intermediate inputs, as users made sure they could obtain those goods. Thus, imports of items whose absence would trigger a large loss of GDP would probably decline by smaller percentages than would imports of other items. Second, to the extent possible, users would make more efficient use of goods that were in short supply.

That number can be used to estimate the cost of a one-week closure of the Los Angeles and Long Beach ports. The value of containerized imports entering through those ports is estimated to total almost $210 billion in 2006. If the backlog of shipments from a closure took three additional weeks to clear, then four weeks of cargo would be delayed overall—the week of cargo during the shutdown and the three following weeks of cargo, which would be delayed by the need for the ports to take care of the backlog. The average delay at the beginning of the three-week clearing period (including cargo that would have arrived on the first day of the disruption) would be seven days, and the average delay at the end would be zero. Therefore, the average number of days of delay for the four weeks of cargo would be 3.5 days. Hence, the total cost of the delay would be about $450 million for an average week, or $65 million per day of closure.

A Three-Year Shutdown of Container Traffic at the Los Angeles and Long Beach Ports

If the ports of Los Angeles and Long Beach were closed for three years, losses of both GDP and imports would be much larger—and would not be recouped after the shutdown. The pattern of losses would vary over time. The market for port services would be tightest during the first year of the disruption. Before shippers and their customers had time to fully adjust to the closure, the reliance on available ports (and the willingness to pay for port services) would be great. Extraordinary adjustments and large cost increases would occur. Imported goods with the lowest value would be likely to stay behind, requiring the greatest response from U.S. producers of substitute goods. Some of the highest-value items would be redirected through East and Gulf Coast ports and to air transport, raising shipping times and costs. All of those adjustments would be costly, so consumers and businesses would have to pay more for imports and for goods produced using imports.

Those cost increases would spur another set of adjustments, as consumers and businesses shifted their demand (to some extent) away from goods whose prices had risen the most and toward goods whose price increases had been more moderate. Consumers would curtail their overall purchases because rising prices would reduce their real income. Companies that relied on imports would look for domestic substitutes, whose production would then increase. Moreover, businesses would alter their investment plans to reflect both the change in demand for their products and the higher cost of their inputs.

With time, the new investments in facilities and intermodal connections with trucking and rail at alternative ports, plus the full reopening of the Los Angeles and Long Beach ports, would allow more imports to enter the United States at lower costs. GDP would almost completely rebound to where it would have been without the port disruption, and national employment would rebound completely. Activity levels at various ports could be somewhat different, however, as could business practices. The Los Angeles and Long Beach ports could permanently lose some business to other

ports that had added capacity. Businesses might decide to carry more inventory to guard against future disruptions in imports.

Diversion Assumptions in the Simulation. To represent shippers' and customers' response to the closure of a port and the likely increases in containerized imports at other ports, CBO assumed that only part of the growing container traffic that normally would have been flowing to Los Angeles and Long Beach (baseline imports) would not enter the United States. Specifically, CBO assumed that:

- In the first year, 35 percent of the baseline imports would arrive elsewhere in the country;
- By the second year, construction of additional port and air-freight capacity would boost that figure to 55 percent; and
- By the third year, 70 percent of that baseline traffic would enter the United States.

Those assumptions are consistent with how much additional traffic the nation's remaining ports might be able to handle, given the likely additions to their capacity and other adjustments. Among the changes that would help to limit import losses, CBO assumed that 5 percent of baseline containerized imports would be diverted, in some combination, to ports in Canada and Mexico (for subsequent import by rail and truck) or would travel instead as bulk cargo or air freight. Even so, the nation's other container ports would have to increase their total intake of containers by about 25 percent over baseline levels in the first year, by 35 percent by the second year, and by 50 percent by the third year. In the first year of the scenario, the one-week national disruption combined with the lengthy closure of Los Angeles and Long Beach would mean that other U.S. ports would need at least three months to clear the backlog from that one week. The backlog also contributes to the especially large loss of imports in that first year.

Exports would also be disrupted by a closure of the Los Angeles and Long Beach ports, although the principal economic effects would result from the disruption of imports. Containerized exports at those two ports are so small ($32 billion in 2004) relative to containerized imports ($182 billion) that constraints on the capacity to move them to other ports and load them on ships are unlikely to be a problem. Thus, CBO assumes that all of those exports could be diverted to other ports.

The cost of transporting those export goods to alternative ports would most likely be greater than the cost of shipping them to Los Angeles and Long Beach. The cost increase would be small, however, because many of the affected commodities are already being transported to the West Coast from other parts of the country.

Simulation Results. In the simulation, the three-year shutdown reduces real GDP by between 0.35 percent and 0.55 percent, or $45 billion to $70 billion, per year. That

translates into daily costs ranging from $125 million to $200 million. Outlays by consumers and businesses fall by substantially more than that, however, because they include less spending on both imported and domestically produced goods, whereas the decline in real GDP reflects only reductions in domestic production.

Inflation—as measured by consumer prices—is about 2 percentage points higher in the first year of the simulation than it would be otherwise, little changed in the second year, and lower thereafter, eventually bringing the level of consumer prices back to where it would have been without the disruption. (Thus, for example, if inflation would have been a steady 2 percent without the port closure, it would rise to 4 percent in the first year of the shutdown, fall back to 2 percent in the second year, and then decline further in the following two years.) Initially, the increase is driven by the constraint on imports. The LIFT model assumes that the effects of that constraint are reflected only slowly in final prices; thus, it may understate the impact on inflation in the first year. However, the slow response of final prices is consistent with recent experience, when core consumer prices did not change significantly in response to the shock of higher energy prices. Inflation declines in the third and fourth years of the simulation (despite the delayed impact of the first year's import shortage) mainly because of the adjustments that are assumed to be made—especially the easing of the shortage through increases in imports at other ports.

An additional 2 percent jump in prices would call for a decision by the Federal Reserve Board about whether to tighten monetary policy to constrain inflation. The usual rules of thumb for monetary policy suggest that interest rates would rise. However, in the simulation, interest rates actually fall slightly in nominal terms, which implies a large reduction in real interest rates and an extremely accommodative monetary policy. Because the increase in inflation would be expected to be temporary, the Federal Reserve might well decide that an accommodative policy was appropriate to minimize losses to GDP and income. If, instead, the Federal Reserve acted more aggressively to suppress the additional inflation, the first-year increase might not be affected much (because of inflation's slow response to monetary policy), but the decline over the next two years would be greater. However, the reduction in real GDP during the three-year shutdown would probably also be larger.

The employment level would be about 1 million jobs lower, on average, over the three-year period than it would be otherwise, according to the simulation. That reduction is large given the reduction in GDP because the jobs that would be lost on account of the closure have, on average, lower pay and productivity and fewer weekly hours than the national averages. However, given uncertainty about the composition of the displaced imports and the response of individual industries to such a disruption, the decline in employment is highly uncertain. In any event, that decline—which equals roughly six months' worth of employment growth—would not be permanent. Employment would rebound as the economy recovered from the disruption.

A loss in GDP would persist after the three-year shutdown, the simulation indicates, though at a much lower level (less than 0.1 percent of GDP in the succeeding two years). That result occurs in part because the decline in investment in the first three years is not fully made up, leaving the economy with a slightly smaller productive capacity.

Sources of Uncertainty. Those simulation results are subject to a great deal of uncertainty, which stems from various sources:

- The ability of importers to find alternative ways to bring products into the United States—through other ports, by air, or even via Canada and Mexico—is unclear. A fuller understanding of the potential for diverting traffic would require a port-by-port analysis of the present spare capacity (including the capacity of intermodal links and of rail and trucking), current plans for expanding capacity, and likely growth in container traffic.

- CBO has no specific knowledge about which industries or companies use just-in-time inventory management and thus could be disproportionately upset by disruptions to imports. Ignoring just-in-time inventory management might, by itself, lead to understating the effects of import disruption. However, CBO has also made no specific assumptions about the ability of importers with high-value goods—such as those destined for just-in-time manufacturers—to get to the head of the line. If high-value imports are less affected and the imports that cannot enter through alternative ports are largely of low value, the simulations may overstate the costs of a port closure. (For the unit values of major imports to Los Angeles and Long Beach, see Table 5.)

- The outcome for GDP will depend in part on the speed with which increases in import prices are reflected in the prices of final goods and on the Federal Reserve's response, both of which are uncertain.

Table 5.

Unit Value of the Top 20 Containerized Imports at Los Angeles and Long Beach Ports, 2004

HS#	Category of Import	Value (Billions of dollars)	Weight (Thousands of short tons)	Unit Value (Thousands of dollars per ton)
84	Machinery, Boilers, Reactors, Parts	38.0	698.6	54.3
85	Electric Machinery, Sound and Television Equipment, Parts	31.7	677.0	46.8
87	Vehicles and Parts, Except Railway or Tramway	12.1	337.4	35.8
62	Apparel Articles and Accessories, Not Knit or Crochet	9.9	132.4	74.6
95	Toys, Games, and Sports Equipment and Parts	9.4	377.1	25.0
94	Furniture, Bedding, Lamps, Etc.	9.3	739.8	12.6
61	Apparel Articles and Accessories, Knit or Crochet	9.0	132.1	68.4
64	Footwear	7.8	181.4	43.0
39	Plastics and Articles Thereof	5.2	409.0	12.8
73	Articles of Iron or Steel	4.4	467.0	9.4
42	Leather Articles, Saddlery, Handbags	3.8	117.2	32.1
90	Optic, Photographic, and Medical Instruments	3.6	41.8	86.2
40	Rubber and Articles Thereof	3.5	207.1	16.7
63	Textile Articles, Needlecraft, Worn Textile Articles	2.6	97.9	26.3
03	Fish, Crustaceans	2.1	86.0	24.5
44	Wood and Wood Articles	1.6	210.0	7.8
83	Miscellaneous Articles of Base Metal	1.6	91.6	17.5
82	Tools, Cutlery, Etc.	1.6	61.4	25.3
48	Paper and Paperboard	1.4	162.7	8.9
72	Iron and Steel	1.3	461.6	2.8
	Total, Top 20 Containerized Imports	**159.9**	**5,689.1**	**n.a.**
All Containerized Imports		**182.3**	**7,465.2**	**n.a.**

Source: Congressional Budget Office based on information from the U.S. Maritime Administration.

Note: HS = Harmonized Commodity Description and Coding System; n.a. = not applicable.

Appendix A: How CBO Estimated the Macroeconomic Effects of a Port Shutdown

To estimate the impact of a disruption to containerized traffic, the Congressional Budget Office (CBO) contracted with Inforum, a nonprofit economic consulting group affiliated with the University of Maryland, to use its LIFT model. LIFT is an interindustry model with full "bottom-up" (commodity-by-commodity) accounting that can be used to examine the macroeconomic effects of industry-specific disruptions to imports. In the model, disruptions to imports of intermediate goods—modeled as increases in the prices of those goods—result in lost domestic production of items that use the goods as inputs. Domestic competitors of foreign suppliers increase production, offsetting some of the reduction in gross domestic product (GDP). Disruptions to imports of final goods result in lower consumption and investment but little net change in GDP.

To estimate the types and values of trade that would be affected by a disruption, CBO's analysis uses 2004 data from the federal government on imports arriving at individual ports by container and arriving nationwide by all modes of transportation—air freight, tankers, containers, bulk cargo, and rail.[1] Imported commodities are categorized according to the Harmonized Commodity Description and Coding System (HS). The data on individual port traffic are available at the 6-digit HS level of detail. Additional data on national imports arriving by all modes are available at the 10-digit HS level. Inforum converts those HS data to Standard Industrial Classification (SIC) codes for interface with the LIFT model.

CBO's analysis of the port-closure scenarios is built on the assumption that imports of specific commodities would decline by the amounts that would have been expected to arrive in Los Angeles and Long Beach. The reductions are net of imports assumed to be diverted to other ports (including some in Canada and Mexico) or arriving by other modes of transportation (including some transshipment to bulk cargo and air freight).[2] One key factor in deciding how much traffic could be diverted to unaffected ports is the reasonableness of the resulting increase in traffic at those ports.

1. Data on trade in goods, by commodity, were provided to CBO by the Foreign Trade Division of the Census Bureau and by the U.S. Maritime Administration.

2. CBO assumed that net containerized imports at U.S. ports (including Los Angeles and Long Beach) would have grown by 7.5 percent annually in 2006 through 2008 in the absence of a shutdown.

In a three-year shutdown, the amount of diversion is assumed to grow each year, consistent with the construction of new capacity at other ports and greater use of alternative modes of transportation. Specifically, CBO assumed that:

- In the first year, 35 percent of the baseline container shipments to the Los Angeles and Long Beach ports would arrive elsewhere in the United States;
- By the second year, that figure would rise to 55 percent with the construction of additional port and air-freight capacity; and
- By the third year, 70 percent of that baseline traffic would enter the country.

To implement the import reductions in the simulations, Inforum raised import prices to the level required to reduce imports of a commodity by the amount assumed in the disruption scenario. That level may not be the price paid by importers, because nonprice rationing, or shortages, might occur during the disruption. Rather, those higher prices represent the "shadow price" of imports—the true cost of imports to their users. Higher shadow prices encourage U.S. consumers and businesses to substitute other goods for scarce imports and encourage U.S. producers to boost output of those items.

Since the shadow price can differ substantially from the actual price received by foreign suppliers, the rise in import prices overstates the total amount that U.S. customers pay to foreign suppliers in the simulations. CBO assumed that only 25 percent of the rise in import prices represents a genuine increase in those prices. The rest is recycled back to the United States through an increase in U.S. income from foreign assets. (Part of the rise in shadow prices can be thought of as an increase in the income of foreign subsidiaries of U.S. firms.)

Appendix B: Disruption of Container Shipments from Hong Kong

Although this report focuses on the consequences of disruptions to U.S. port activity, events that forced the closure of major foreign ports would also be of concern to the United States. The impact on U.S. consumption or production would depend on the value of the goods that were not delivered to the United States, regardless of where the supply chain was interrupted.

Some people have expressed specific concern about the effects of a closure of Hong Kong, the largest container port in the world (see Figure B-1). However, the opportunities to divert traffic around Hong Kong appear to be substantial, which would diminish the impact of a shutdown of that port.

Hong Kong (including the cities of Hong Kong and Kowloon) is the biggest single source of container shipments to the United States. In 2004, $43.4 billion in containerized imports arrived in the United States from Hong Kong. They accounted for about 10 percent of all containerized imports to the United States and about 3 percent of total U.S. imports of goods.

Those figures overstate the importance of Hong Kong as a source of U.S. imports, however. Hong Kong is a major location for transshipment—nearly 90 percent of the containerized goods leaving that port originated elsewhere (see Table B-1). Containerized goods and bulk cargoes arrive in Hong Kong from other ports in Asia, generally on relatively small vessels, and by land from elsewhere in China. Those shipments are consolidated and loaded onto very large container ships for the journey to North America and elsewhere.

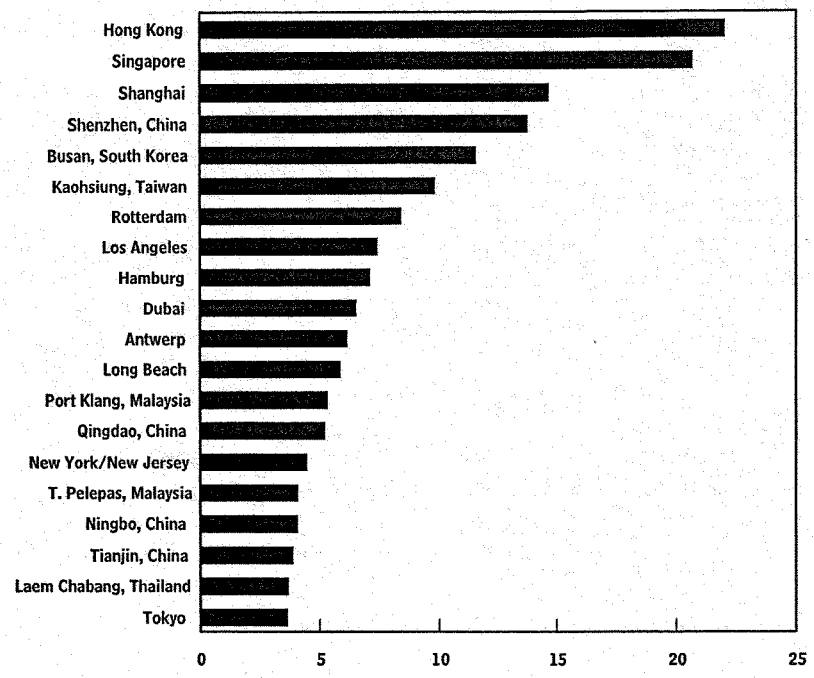
Any closure of Hong Kong would probably force other ports in the region to take on more of the task of consolidating shipments. In addition, many container shipments to the United States and other destinations would most likely forgo transshipment altogether, traveling on smaller vessels than would otherwise be the case.

Thirteen of the world's top 20 ports for container shipments are located in Asia; thus, the opportunities for other regional ports to compensate for a closure of Hong Kong are significant. Moreover, those ports are already competing aggressively with Hong Kong for additional business. All of them have rapidly expanded the capacity to handle containers in recent years. Judging by 2005 traffic levels, if all Hong Kong container traffic was diverted to the closest top-20 ports (in Singapore, China, South Korea, Taiwan, and Japan), shipments from those ports would increase by 25 percent.

Figure B-1.

Containerized Imports and Exports from the World's 20 Largest Ports, 2004

(Millions of 20-foot equivalent units)



Source: Congressional Budget Office using data from Bloomberg.com, "Hong Kong Trails Singapore in 2005 Container Volume" (January 16, 2006), available at www.bloomberg.com/apps/news?pid=10000080&refer=asia&sid=aPIM0vYUVhbQ#.

Note: Marine containers come in various sizes. To allow for consistency in comparisons, those sizes are commonly presented in terms of a standard 20-foot container. For example, one 40-foot container would be counted as two 20-foot equivalent units.

For those reasons, a closure of Hong Kong could raise the cost of shipping goods to the United States, but it would be unlikely to curtail shipments significantly. The cost increase would be lower if additional diversion occurred to smaller ports in Asia. If an increased percentage of available container space was used for goods with the highest value—as would be likely—the economic impact on the United States would be lower still.

Table B-1.

Top 20 Containerized Imports to the United States, by Value, That Passed Through or Originated in Hong Kong, 2004

(Billions of dollars)

HS#	Category of Import	Total Containerized Imports from Hong Kong	Total Originating in Hong Kong	Total Transshiped from Hong Kong	Percentage Transshiped
85	Electric Machinery, Sound and Television Equipment, Parts	8.5	0.7	7.9	92.3
95	Toys, Games, and Sports Equipment and Parts	6.3	0.2	6.1	96.9
84	Machinery, Boilers, Reactors, Parts	3.9	0.2	3.7	94.7
61	Apparel Articles and Accessories, Knit or Crochet	3.9	1.3	2.6	65.8
64	Footwear	3.8	0.1	3.7	97.9
62	Apparel Articles and Accessories, Not Knit or Crochet	3.4	1.4	2.0	57.8
94	Furniture, Bedding, Lamps, Etc.	2.2	0.1	2.1	93.8
42	Leather Articles, Saddlery, Handbags	2.1	0.1	2.0	95.1
39	Plastics and Articles Thereof	1.4	0.2	1.2	86.6
49	Printed Books, Newspapers, Etc.	0.8	0.2	0.6	73.0
90	Optic, Photographic, and Medical Instruments	0.7	*	0.7	93.3
73	Articles of Iron or Steel	0.5	0.1	0.5	89.7
67	Prepared Feathers, Down, Etc.	0.5	*	0.5	96.7
83	Miscellaneous Articles of Base Metal	0.5	*	0.5	91.5
48	Paper and Paperboard	0.5	0.1	0.4	88.3
91	Clocks and Watches and Parts	0.4	*	0.4	95.1
63	Textile Articles, Needlecraft, Worn Textile Articles	0.4	*	0.4	93.1
96	Miscellaneous Manufactured Articles	0.3	*	0.3	89.1
87	Vehicles and Parts, Except Railway or Tramway	0.3	*	0.3	86.4
82	Tools, Cutlery, Etc.	0.3	*	0.2	92.7
	Total, Top 20 Containerized Imports	**40.8**	**4.9**	**35.9**	**88.0**
All Containerized Imports		**43.4**	**5.3**	**38.1**	**87.8**

Source: Congressional Budget Office based on data from the U.S. Maritime Administration.

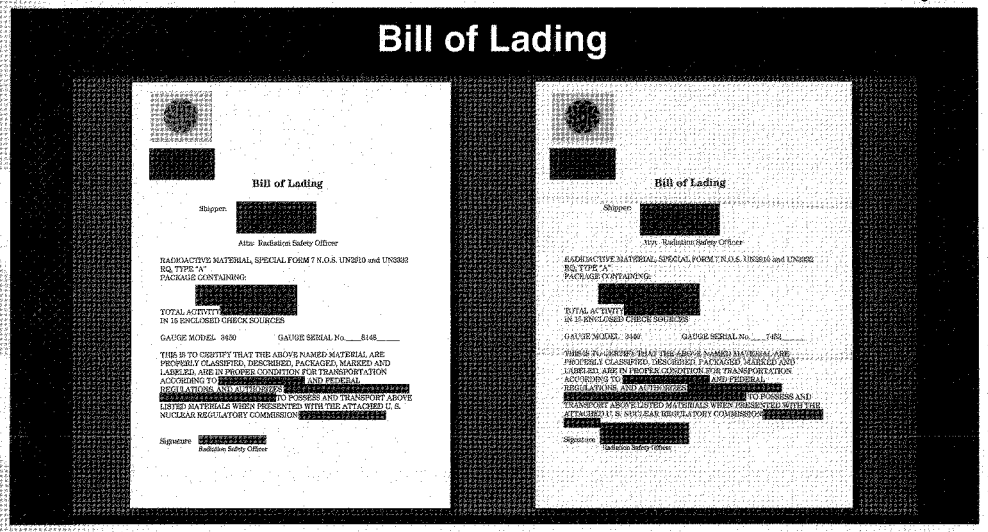
Note: HS = Harmonized Commodity Description and Coding System; * = less than $50 million.

GAO
Accountability * Integrity * Reliability
Office of Forensic Audits and Special Investigations
Boxes Containing Radioactive Material
Permanent Subcommittee on Investigations
EXHIBIT #10

GAO
Accountability * Integrity * Reliability

Office of Forensic Audits and Special Investigations

Bill of Lading



Bill of Lading

Shipper:

Attn: Radiation Safety Officer

RADIOACTIVE MATERIAL, SPECIAL FORM 7 N.O.S. UN2910 and UN3332
RQ, TYPE "A"
PACKAGE CONTAINING:

TOTAL ACTIVITY
IN 15 ENCLOSED CHECK SOURCES

GAUGE MODEL 3430 GAUGE SERIAL No.___8148_____

THIS IS TO CERTIFY THAT THE ABOVE NAMED MATERIAL ARE PROPERLY CLASSIFIED, DESCRIBED, PACKAGED, MARKED AND LABELED, ARE IN PROPER CONDITION FOR TRANSPORTATION ACCORDING TO [redacted] AND FEDERAL REGULATIONS, AND AUTHORIZES [redacted] TO POSSESS AND TRANSPORT ABOVE LISTED MATERIALS WHEN PRESENTED WITH THE ATTACHED U. S. NUCLEAR REGULATORY COMMISSION [redacted]

Signature [redacted]
Radiation Safety Officer

Bill of Lading

Shipper:

Attn: Radiation Safety Officer

RADIOACTIVE MATERIAL, SPECIAL FORM 7 N.O.S. UN2910 and UN3332
RQ, TYPE "A"
PACKAGE CONTAINING:

TOTAL ACTIVITY
IN 15 ENCLOSED CHECK SOURCES

GAUGE MODEL 3440 GAUGE SERIAL No.___7452____

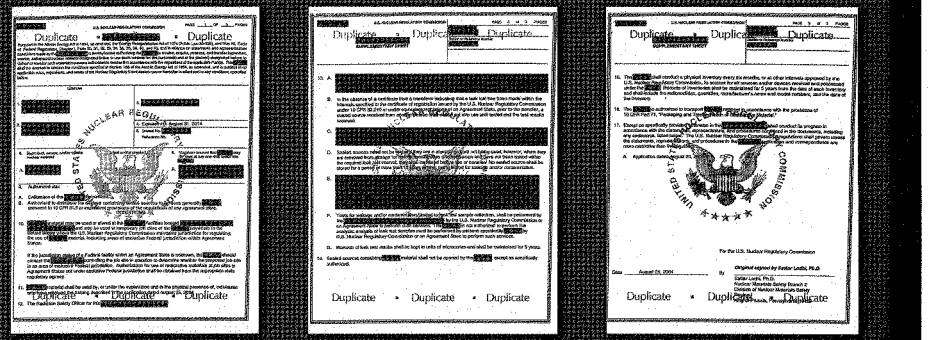
THIS IS TO CERTIFY THAT THE ABOVE NAMED MATERIAL ARE PROPERLY CLASSIFIED, DESCRIBED, PACKAGED, MARKED AND LABELED, ARE IN PROPER CONDITION FOR TRANSPORTATION ACCORDING TO [redacted] AND FEDERAL REGULATIONS, AND AUTHORIZES [redacted] TO POSSESS AND TRANSPORT ABOVE LISTED MATERIALS WHEN PRESENTED WITH THE ATTACHED U. S. NUCLEAR REGULATORY COMMISSION [redacted]

Signature [redacted]
Radiation Safety Officer

GAO
Accountability * Integrity * Reliability

Office of Forensic Audits and Special Investigations

Nuclear Regulatory Commission Document



United States Government Accountability Office

GAO

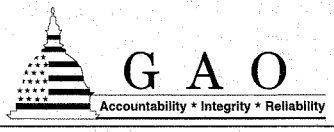
Statement for the Record to the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EST
Thursday, March 30, 2006

CARGO CONTAINER INSPECTIONS

Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System

Statement for the Record by Richard M. Stana, Director
Homeland Security and Justice Issues



GAO-06-591T

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-591T, a statement for the record to the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate

Why GAO Did This Study

U.S. Customs and Border Protection's (CBP) Automated Targeting System (ATS)—a computerized model that CBP officers use as a decision support tool to help them target oceangoing cargo containers for inspection—is part of CBP's layered approach to securing oceangoing cargo. GAO reported in February 2004 on challenges CBP faced in targeting oceangoing cargo containers for inspection and testified before this subcommittee in March 2004 about the findings in that report. The report and testimony outlined recommendations aimed at (1) better incorporating recognized modeling practices into CBP's targeting strategy, (2) periodically adjusting the targeting strategy to respond to findings that occur during the course of its operation, and (3) improving implementation of the targeting strategy. This statement for the record discusses preliminary observations from GAO's ongoing work related to ATS and GAO's 2004 recommendations addressing the following questions:

- What controls does CBP have in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of smuggled weapons of mass destruction?
- How does CBP systematically analyze security inspection results and incorporate them into ATS?
- What steps has CBP taken to better implement the rest of its targeting strategy at the seaports?

www.gao.gov/cgi-bin/getrpt?GAO-06-591T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Richard Stana at (202) 512-8777 or stanar@gao.gov.

March 30, 2006

CARGO CONTAINER INSPECTIONS

Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System

What GAO Found

CBP has not yet put key controls in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction. To provide assurance that ATS targets the highest-risk cargo containers as intended, CBP is (1) working to develop and implement performance measures related to the targeting of cargo containers, (2) planning to compare the results of its random inspections with its ATS inspection results, (3) working to develop and implement a testing and simulation environment, and (4) addressing recommendations contained in a 2005 peer review of ATS. CBP expects to begin using performance measures in June 2006 and enter the final phase of software development for its testing and simulation environment at the same time. However, to date, none of these four initiatives has been fully implemented. Thus, CBP does not yet have key internal controls in place to be reasonably confident that ATS is providing the best information to allocate resources for targeting and inspecting containers that are the highest risk and not overlook inspecting containers that pose a threat to the nation.

CBP does not yet have a comprehensive, integrated system in place to analyze security inspection results and incorporate them into ATS. CBP currently adjusts ATS based on intelligence information it receives and has initiated a process to track suggestions submitted by CBP targeting officers at the seaports for modifying ATS. However, CBP has not yet implemented plans to refine ATS based on findings from routine security inspections. Without a more comprehensive feedback system, CBP is limited in refining ATS, a fact that could hinder the overall effectiveness of the targeting strategy.

CBP has taken steps to improve implementation of the targeting strategy at the seaports. It has implemented a testing and certification process for its officers who complete the Sea Cargo Targeting Course that should provide better assurance of effective targeting practices. CBP has also made a good faith effort to address longshoremen's safety concerns regarding radiation emitted by nonintrusive inspection equipment by taking actions such as working with longshoremen's unions and other maritime organization to develop public radiation tests on the nonintrusive inspection equipment. Nevertheless, CBP has not been able to persuade one longshoremen's union to permit changes in the procedure for staging containers to increase inspection efficiency at some West Coast seaports where the union's members work.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to comment on our ongoing work on the U.S. Customs and Border Protection's (CBP) Automated Targeting System (ATS)—a computerized model that CBP officers use as a decision support tool to help them target oceangoing cargo containers for inspection.[1]

In the aftermath of the terrorist attacks of September 11, 2001, there is heightened concern that terrorists will attempt to smuggle a weapon of mass destruction (e.g., a nuclear, biological, or radiological explosive device) into the United States using one of the 11 million cargo containers that arrive at our nation's seaports. Because of the large volume of imported containers, CBP maintains that it is unable to physically inspect all oceangoing containers without disrupting the flow of commerce. Thus, CBP uses a multilayered strategy for addressing the threat posed by the movement of oceangoing containers, of which ATS is a key component.[2] CBP uses ATS to review documentation and assign a risk score for all containers destined for U.S. ports. CBP officers located at domestic ports or at 1 of the 40 foreign ports that participate in the Container Security Initiative (CSI) then use these scores to help them make decisions on the extent of additional documentary review and possible physical inspection that will be conducted at the seaport.

We previously reported in February 2004 on the challenges CBP faced in targeting oceangoing cargo containers for inspection[3] and testified before this Subcommittee in March 2004 about the findings in that report.[4] The

[1]A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.

[2]In addition to ATS, CBP's multilayered strategy includes the (1) Compliance Measurement Program, which randomly selects additional containers to be physically examined; (2) the Container Security Initiative, whereby CBP places staff at foreign seaports to work with foreign counterparts to inspect high-risk containers before they are shipped to the United States; and (3) the Customs-Trade Partnership Against Terrorism which is a cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains. A supply chain consists of all stages involved in fulfilling a customer request, including stages conducted by manufacturers, suppliers, transporters, retailers, and customers.

[3]GAO, *Homeland Security: Challenges Remain in the Targeting of Oceangoing Cargo Containers for Inspection*, GAO-04-352NI (Washington, D.C.: Feb. 20, 2004).

[4]GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T, (Washington, D.C.: Mar. 31, 2004).

report and testimony outlined recommendations aimed at (1) incorporating recognized modeling practices into its targeting strategy, such as conducting simulated events and initiating an external peer review,[5] (2) periodically adjusting the targeting strategy to respond to findings that occur during the course of its operation, and (3) improving implementation of the targeting strategy at domestic seaports. This subcommittee and other congressional requesters asked that we ascertain whether CBP had implemented the recommendations we made to improve the targeting strategy. Our work, in response to this request, has been under way since last October, and we expect to complete the work and provide this subcommittee and our other requesters with a report on the final results later this year. In this statement, I will discuss our preliminary observations on the status of these recommendations as part of the following questions:

- What controls does CBP have in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of smuggled weapons of mass destruction?
- How does CBP systematically analyze security inspection results and incorporate them into ATS?
- What steps has CBP taken to better implement the rest of its targeting strategy at the seaports?

To address these questions, we interviewed CBP officials in headquarters and visited six seaports: Baltimore, Charleston, Los Angeles-Long Beach, Miami, New York-New Jersey, and Savannah. Because we did not select a random sample of ports to visit, the results from these visits cannot be generalized to ports nationwide. We also met with CBP's contractor responsible for conducting CBP's peer review of ATS and longshoremen's union representatives. We reviewed CBP's policies and procedures for targeting and inspecting shipments, and its documentation on intelligence gathering and dissemination, targeting strategies, random inspections, training, and radiation safety as well as its peer review report. We also examined information on officers trained and certified in CBP's Sea Cargo Targeting Training course. We did not independently validate the reliability of CBP's targeting results or test the effectiveness of ATS. We conducted our work in response to this request from October 2005 through March 2006 in accordance with generally accepted government

[5]External peer review is a process that includes an assessment of the model by independent and qualified external peers.

auditing standards. Appendix I contains more detailed information on our scope and methodology.

Summary

CBP has not yet put key controls in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction.[6] To provide assurance that ATS targets the highest-risk cargo containers as intended, CBP is (1) working to develop and implement performance measures related to the targeting of cargo containers, (2) planning to compare the results of its random inspections with its ATS inspection results, (3) working to develop and implement a testing and simulation environment, and (4) addressing recommendations contained in a 2005 peer review of ATS. CBP expects to begin using performance measures in June 2006 and enter the final phase of software development for its testing and simulation environment at the same time. However, to date, none of these four initiatives has been fully implemented. Thus, CBP does not yet have key internal controls in place to be reasonably confident that ATS is providing the best information to allocate resources for targeting and inspecting containers that are the highest risk and not overlook inspecting containers that pose a threat to the nation.[7]

CBP does not yet have a comprehensive, integrated system in place to analyze security inspection results and incorporate them into ATS. An integrated system would allow any of the various systems that CBP uses to manage cargo inspection data to communicate with one another for the purpose of analyzing combined data. CBP currently adjusts ATS based on intelligence information it receives and has initiated a process to track suggestions submitted by CBP targeting officers at the seaports for modifying ATS. However, CBP has not yet implemented plans to refine ATS based on findings from routine security inspections. Without a more comprehensive feedback system, CBP is limited in refining ATS, a fact that could hinder the overall effectiveness of the targeting strategy.

[6]For purposes of this statement, when we state that CBP uses ATS to target oceangoing cargo containers to identify weapons of mass destruction, we are also including the different components that could be used to create a weapon of mass destruction.

[7]Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations.

CBP has taken steps to improve implementation of the targeting strategy at the seaports. It has implemented a testing and certification process for its officers who complete the Sea Cargo Targeting Course that should provide better assurance of effective targeting practices. CBP has also made a good faith effort to address longshoremen's safety concerns regarding radiation emitted by nonintrusive inspection equipment by taking actions such as working with longshoremen's unions and other maritime organization to develop public radiation tests on the nonintrusive inspection equipment.[8] Nevertheless, CBP has not been able to persuade one longshoremen's union to permit changes in the procedure for staging containers to increase inspection efficiency at some West Coast seaports where the union's members work.

Background

Oceangoing cargo containers have an important role in the movement of cargo between global trading partners. Approximately 90 percent of the world's trade is transported in cargo containers. In the United States almost half of incoming trade (by value) arrives by containers aboard ships. If terrorists smuggled a weapon of mass destruction into the nation using a cargo container and detonated such a weapon at a seaport, the incident could cause widespread death and damage to the immediate area, perhaps shut down seaports nationwide, cost the U.S. economy billions of dollars, and seriously hamper international trade.

The Department of Homeland Security and CBP are responsible for addressing the threat posed by terrorist smuggling of weapons in oceangoing containers. To carry out this responsibility, CBP uses a layered security strategy. One key element of this strategy is ATS. CBP uses ATS to review documentation, including electronic manifest information submitted by the ocean carriers on all arriving shipments, to help identify containers for additional inspection.[9] CBP requires the carriers to submit manifest information 24 hours prior to a United States-bound sea container being loaded onto a vessel in a foreign port. ATS is a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment in a container based on manifest information. As previously discussed, CBP officers use these scores to help them make

[8]Nonintrusive inspection equipment uses technology to help determine the contents of a container without opening it.

[9]Cargo manifests are prepared by the ocean carrier to describe the contents of a container.

decisions on the extent of documentary review or physical inspection to be conducted.

ATS is an important part of other layers in the security strategy. Under its CSI program, CBP places staff at designated foreign seaports to work with foreign counterparts to identify and inspect high-risk containers for weapons of mass destruction before they are shipped to the United States. At these foreign seaports, CBP officials use ATS to help target shipments for inspection by foreign customs officials prior to departing for the United States. Approximately 73 percent of cargo containers destined for the United States originate in or go through CSI ports.

ATS is also an important factor in the Customs-Trade Partnership Against Terrorism (C-TPAT) program. C-TPAT is a cooperative program linking CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected. Specifically, C-TPAT members receive a range of benefits, some of which could change the ATS risk characterization of their shipments, thereby reducing the probability of extensive documentary and physical inspection.

CBP Currently Does Not Have Reasonable Assurance That ATS Is Effective

CBP does not yet have key controls in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction. To address this shortcoming, CBP is (1) developing and implementing performance metrics to measure the effectives of ATS, (2) planning to compare the results of randomly conducted inspections with the results of its ATS inspections, (3) developing and implementing a simulation and testing environment, and (4) addressing recommendations contained in a 2005 peer review. To date, none of these control activities have been fully completed or implemented.[10] Thus, CBP does not yet have key internal controls in place to be reasonably certain that ATS is providing the best available information to allocate resources for targeting and inspecting

[10]The Comptroller General's internal control standards state that internal control activities help ensure that management's directives are carried out. Further, they state that the control activities should be effective and efficient in accomplishing the agency's control objectives. GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1, p. 11 (Washington, D.C.: November 1999).

containers that are the highest risk and thus not overlook inspecting containers that pose a high threat to the nation.

CBP Does Not Yet Have Performance Measures to Gauge the Effectiveness of ATS in Targeting Cargo Containers, But is Working to Develop Them

CBP does not yet have performance measures in place to help it determine the effectiveness of ATS at targeting oceangoing cargo containers with the highest risk of smuggled weapons of mass destruction. The Comptroller General's internal control standards include the establishment and review of performance measures as one example of a control activity to help an entity ensure it is achieving effective results.[11] In July 2005, CBP contracted with a consulting firm to develop such performance metrics. CBP officials and personnel from this consulting firm told us that the firm's personnel analyzed shipment information in ATS over a 2-year period to obtain additional insights into ATS's performance and to determine whether ATS is more effective at targeting cargo containers for terrorism related risk than a random sampling inspection approach. CBP officials told us that the consulting firm's personnel prepared a draft of the results of their analyses and that, as of March 21, 2006, CBP officials are reviewing these analyses. They also said that the consulting firm's personnel are documenting the methodology for their analyses and related performance measures that CBP can use in the future. CBP officials expect to receive this methodology and the performance measures in April 2006, and told us that they expect to begin using the measures in June 2006. CBP officials also told us that they initially planned to have performance measures developed by August 31, 2005, but that this process has taken longer than expected because of delays in (1) obtaining security clearances for the consulting firm's personnel, (2) obtaining workspace for the firm's staff, and (3) arranging for the appropriate levels of access to CBP's information systems.

CBP Is Not Yet Using the Results of Random Inspections to Assess ATS Effectiveness

Currently, CBP is not using the results of its random sampling program to assess the effectiveness of ATS. As part of its Compliance Measurement Program, CBP plans to randomly select 30,000 shipments based on entry information submitted by the trade community and examine those

[11]See GAO/AIMD-00-21.3.1, pps. 11 and 14.

shipments to ensure compliance with supply chain security during fiscal year 2006.[12]

At this time, CBP is unable to compare the examination results from its random sampling program with its ATS inspection results, as we recommended in our 2004, report because CBP does not yet have an integrated, comprehensive system in place to compare multiple sets of data—like results of random inspections with results of routine ATS inspections that were triggered by ATS scores and other operational circumstances. Such a comparison would allow examination of if and why the outcomes of ATS's weighted rule sets are not consistent with the expected outcomes possible in the universe of cargo containers, based on sample projections. Furthermore, the Comptroller General's standards for internal control state that information should be recorded and communicated to management and others within the entity who need it in a form that enables them to carry out their responsibilities.[13]

CBP Has Not Yet Tested the Effectiveness of ATS in Targeting Cargo Containers for Inspection but Has Plans to Do So

Currently, CBP does not conduct simulated events (e.g., covert tests and computer-generated simulations)—a key control activity—to test and validate the effectiveness of ATS in targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction and has not yet implemented a dedicated simulation and testing environment. Without testing and validation, CBP lacks a vital mechanism for evaluating ATS's ability to identify high-risk containers.

In July 2005, CBP contracted with a consulting firm to obtain assistance in the development of a computer-generated simulation and testing environment. CBP officials report that they have the simulation environment infrastructure in place and have processed mock manifest data to simulate cargo linked to terrorism in the new environment. CBP is currently reviewing the results of this test. Further, CBP officials told us that the consulting firm is continuing to work with CBP to develop system requirements so that officers can effectively use the simulation environment. CBP expects to receive the consulting firm's final input for the simulation and testing environment by June 2006. CBP officials said

[12]Entry information is documentation to declare items arriving in the United States. Entry information allows CBP to determine what is included in a shipment. Entry information provides more detail on a container's contents than manifest information.

[13]See GAO/AIMD-00-21.3.1, p. 18.

that they cannot estimate when this simulation and testing environment will be fully operational until CBP receives the consulting firm's final product. As with the development of performance measures, CBP officials also told us that this process has taken longer than expected because of delays in (1) obtaining security clearances for the consulting firm's personnel, (2) obtaining workspace for the firm's staff, and (3) arranging for the appropriate levels of access to CBP's information systems.

As we reported in 2004, terrorism experts suggested that testing ATS by covertly simulating a realistic event using probable methods of attack would give CBP an opportunity to examine how ATS would perform in an actual terrorist situation.[14] CBP officials told us that although they are considering implementing this kind of practice, they do not currently have a program in place to conduct such tests. The Director of CBP's Management Inspections and Integrity Assurance office told us that in mid-April 2006, his office will be presenting a proposal to the Acting Commissioner and other senior management to request initiation of a program to conduct testing of the CSI program that will include testing ATS to help ensure that it is appropriately targeting the highest-risk cargo in the CSI program.

CBP Is Working to Address Peer Review Recommendations

In response to our 2004 recommendation that CBP initiate an external peer review of ATS, CBP contracted with a consulting firm to evaluate CBP's targeting methodology and recommend improvements.[15] Specifically, the contractor identified strengths of the CBP targeting methodology and compared ATS with other targeting methodologies. However, the peer review did not evaluate the overall effectiveness of ATS because CBP did not have the systems in place to allow the contractor to do so.

The contractor's final report, issued in April 2005, identified many strengths in the ATS targeting methodology, such as a very capable and highly dedicated team and the application of a layered approach to targeting. It also made several recommendations to improve the targeting methodology that included control activities, such as (1) the development of performance measures, (2) the development of a simulation and testing environment, (3) the development and implementation of a structured

[14]See GAO-04-352NI.

[15]See GAO-04-352NI.

plan for continual rules enhancement, and (4) an evaluation and determination of the effectiveness of the ATS targeting rules, several of which reinforced the recommendations we made in our 2004 report.[16]

CBP issued a detailed plan, which projected delivery dates, for responding to the recommendations made in the contractor's final report. However, about half of these dates have not been met. For example, CBP projected that it would have its testing and simulation environment in place by September 30, 2005. Although CBP has been working on this effort, the environment has not yet been implemented. As previously discussed, CBP officials said that they cannot provide a current estimate of when this simulation and testing environment will be fully operational.

Although CBP Strives to Refine ATS for Intelligence Information and Officer Feedback, It Is Not Yet Positioned to Use Inspection Results

CBP strives to refine ATS to include intelligence information it acquires and feedback it receives from its targeting officers at the seaports, but it is not able to systematically adjust ATS for inspection results. CBP does not have a comprehensive, integrated system in place to report details on security inspections nationwide that will allow management to analyze those inspections and refine ATS. CBP officials said that they are developing a system that will allow them to do so but did not know when it will be fully operational. CBP officials cautioned that because an inspection does not identify any contraband or a weapon of mass destruction or its components, it may not necessarily indicate that a particular rule is not operating as intended. They noted that terrorist incidents may happen infrequently, and the rule therefore might operate only when weapons, materials, or other dangerous contraband is actually shipped. However, without analyzing and using security inspection results to adjust ATS, CBP is limited in refining ATS, a fact that could hinder the effectiveness of CBP's overall targeting strategy.

CBP Adjusts ATS for Targeting Cargo Containers for Inspection Based on Intelligence

CBP adjusts ATS's rules and weights for targeting cargo containers for inspection in response to intelligence received on an ongoing basis. CBP's Office of Intelligence (OINT) is responsible for acquiring, reviewing, analyzing, and disseminating intelligence. OINT officials told us they receive information from the intelligence community, which includes federal agencies such as the Central Intelligence Agency and the Federal

[16]See GAO-04-352NI.

Bureau of Investigation.[17] According to OINT officials, OINT disseminates information to CBP's offices at the seaports to, among other things, support these offices' targeting efforts related to cargo containers. For example, the targeting officers may use information provided by OINT to search ATS for information about shipments and containers. OINT officials said they also disseminate information to CBP's senior management to inform them about risks associated with cargo containers. CBP uses intelligence information to refine its targeting of cargo containers for inspection by incorporating the intelligence information into ATS to readily identify containers whose manifest information may match or be similar to data contained in the intelligence information.

CBP documentation and our observations showed that CBP headquarters personnel incorporate intelligence information into ATS by adjusting ATS's existing rules and weights and creating new rules and weights that result in a higher risk score being assigned to a container whose manifest information may match or be similar to data contained in the intelligence information. CBP officers can also conduct queries or create lookouts in ATS that will search all manifest data in the system to identify those containers whose manifest information may match or be similar to data contained in the intelligence information.[18] Once ATS identifies these containers, CBP officers are to then designate these containers for inspection. When CBP receives credible intelligence information that requires immediate action, CBP officials also report that they can initiate a special operation to address specific concerns identified in the intelligence data. CBP officials at the six seaports we visited reported that they sometimes receive intelligence information from local sources such as state and local law enforcement. Officials at five of these seaports reported that they will use such information to help them make decisions regarding targeting efforts. Additionally, officials at five of the six seaports we visited said that if the information they receive has national

[17]The intelligence community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

[18]A query is a search an individual officer creates to seek information from ATS about shipments and containers based on specific criteria to assist in the officer's targeting decisions. A lookout is a query that CBP headquarters or officers at the seaports can create that will notify all officers making targeting decisions when a shipment's manifest data are similar to or match the search criteria.

implications, they will notify CBP headquarters personnel, who will make a determination regarding potential adjustments to ATS.

CBP Targeting Officers at the Seaports Have Provided Few Suggestions for Adjusting ATS

In the late summer of 2005, CBP headquarters initiated a process to formally track its targeting officers' suggestions to enhance ATS for targeting cargo containers for inspection. Targeting officers at all six seaports we have visited are aware of the process for providing suggestions to CBP headquarters. According to documentation maintained by headquarters, CBP officers at the seaports have provided few suggestions to date.

CBP headquarters officials said that although they have received few suggestions for modifying ATS, they do not believe this is an indication of ATS's effectiveness. These officials stated that overall the feedback they have received from CBP targeting officers at the seaports related to the operation and usefulness of ATS has been positive.

We reviewed the report CBP uses to track these suggestions and found that since it was established, CBP headquarters has received 20 suggestions for enhancing the ATS component responsible for targeting oceangoing cargo containers for inspection. Some of these suggestions relate to modifying ATS's rules, while others focused on other aspects of ATS such as enhancing the organization and presentation of ATS screens by changing the size of an icon and the fonts or text used.

CBP Is Not Using Inspection Results to Systematically Adjust ATS, but It Is Developing a System to Allow it to Do So

CBP is not using inspection results to systematically adjust ATS for targeting cargo containers for inspection because CBP does not yet have a comprehensive, integrated system in place that can report sufficient details for analyzing inspection results. CBP officials said that although they can analyze inspection results on a case-by-case basis to identify opportunities to refine ATS, such as when an inspection results in a seizure of some type of contraband, they currently do not have a reporting mechanism in place that will allow them to view inspection results nationwide to identify patterns for systematically adjusting ATS. CBP is developing the Cargo Enforcement Reporting Tracking System (CERTS) to document, among other things, all cargo examinations so that documentation substantiating the examinations will be available for analysis by management to adjust ATS. CBP officials said they will begin testing CERTS in the spring of 2006. CBP officials told us that once testing of CERTS is complete, they will be in a better position to estimate when CERTS can be fully implemented.

CBP officials cautioned that because an inspection does not identify any contraband or a weapon of mass destruction or its components, it may not necessarily indicate that a particular rule is not operating as intended. They noted that terrorist incidents may happen infrequently and the rule therefore might operate only when weapons, materials, or other dangerous contraband is actually shipped. However, without using inspection results to adjust ATS, CBP may not be targeting and inspecting containers with the highest risk of containing smuggled weapons of mass destruction.

CBP Has Taken Steps to Better Implement the Targeting Strategy at the Seaports

CBP has implemented a testing and certification process for its officers who complete the Sea Cargo Targeting Course that should provide better assurance of effective targeting practices. CBP has also made a good faith effort to address longshoremen's safety concerns regarding radiation emitted by nonintrusive inspection equipment. Nevertheless, it has not been able to persuade one longshoremen's union to permit changes in the procedure for staging containers to increase inspection efficiency.

CPB Has Implemented a Testing and Certification Process for Officers Who Target Cargo Containers for Inspection

In our 2004 report, we recommended that CBP establish a testing and certification process for CBP staff who complete the national targeting training to provide reasonable assurance that they have sufficient expertise to perform targeting work. [19] CBP has implemented such a testing and certification process.

CBP conducted two evaluations that assessed its targeting training program—a job performance assessment and a job task analysis. With the results of these evaluations, CBP concluded that a certification component should be added to the training program and the Sea Cargo Targeting Training course content should remain unchanged. CBP officials then updated the course materials to encompass the inclusion of the certification component. In October 2004, CBP began certifying officers who successfully completed the Sea Cargo Targeting Training course. Since the establishment of the testing and certification component for the Sea Cargo Targeting Training course, CBP data indicate that it has trained

[19]See GAO-04-352NI.

and certified 278 of its officers responsible for targeting cargo as of March 24, 2006.[20]

While CBP has conducted a job performance assessment prior to the incorporation of a certification program for Sea Cargo Targeting Training, it has not yet formally assessed the impact that revised training and certification has had on officers' targeting of oceangoing cargo containers. However, a CBP official said that CBP has recently initiated planning efforts to begin such an evaluation and expects to complete the evaluation in May 2006. Nevertheless, supervisory officers from five of the six CBP offices at the seaports we visited said that the mandatory training and certification program has been beneficial. These supervisory officers told us that the training and certification improves the confidence of targeters, provides the ability for officers to improve their targeting productivity, and provides an opportunity for officers to gain a broader perspective into the targeting environment by examining passenger and outbound targeting.

Despite CBP Action to Address Longshoremen's Safety Concerns, Efficiency Concerns Remain on the West Coast

In our 2004 report,[21] we discussed concerns that longshoremen had regarding the safety of driving cargo containers through the gamma ray imaging system, one type of nonintrusive inspection equipment used to examine containers to detect potential contraband or weapons of mass destruction. Because this equipment emits radiation as it takes images of the inside of cargo containers, some longshoremen expressed concerns about the health effects of this radiation. As a result of these safety concerns, the longshoremen's union representing West Coast longshoremen established a policy that prevents its members from driving containers through the gamma ray imaging system. In response, CBP altered its procedures at ports affected by this policy. For example, at some West Coast ports, CBP allows longshoremen to stage cargo containers away from the dock, in rows at port terminals, so that CBP officers can then drive the gamma ray imaging system over a group of containers.

[20]A CBP official estimated that CBP has approximately 300 officers responsible for targeting oceangoing cargo containers. However, CBP is currently surveying its offices to determine a more precise estimate and will have this information available within the next month.

[21]See GAO-04-352NI.

However, this procedure can be space-intensive and time-consuming compared to the procedure utilized at East and Gulf Coast ports, whereby the gamma ray imaging system machinery is operated by a CBP officer and parked in place while longshoremen drive the cargo containers through the machinery.[22] At other West Coast ports, the longshoremen get out of the trucks after transporting the cargo containers so that CBP officials can drive the gamma ray imaging system cargo over the container. This is also time-consuming compared to the procedure utilized at the East and Gulf Coast ports.

In response to our recommendation that CBP work with longshoremen to address their safety concerns, CBP engaged in two efforts: (1) establishing CBP's radiation threshold in accordance with the Nuclear Regulatory Commission's (NRC) federal guidelines for public radiation exposure and advertising this threshold to longshoremen through the unions, and (2) working with longshoremen's unions and other maritime organizations to develop public radiation tests on nonintrusive inspection equipment. Officials from the West Coast union that prohibits its members from driving through the gamma ray imaging system told us that the union is satisfied with CBP efforts to operate the gamma ray imaging system in an alternative format, to comply with the union's policy of receiving no amount of man-made radiation. Despite CBP efforts to assure this union that the amount of radiation emitted by the gamma ray imaging system is within safe levels, a union representative told us that CBP will not convince the union to change its policy unless it eliminates radiation emission from inspection equipment.

- - - - -

In closing, ATS is an integral part of CBP's layered security strategy. A well-functioning ATS is crucial to the effective screening of cargo containers at domestic and CSI foreign ports, as well as cargo shipped by the trade community participating in C-TPAT. While CBP is working to make improvements to ATS, our ongoing work indicates that it is not yet in a position to gauge the effectiveness of ATS. We are continuing to review CBP's plans and actions to improve ATS and will report to this subcommittee and the other requesters later this year.

[22]See GAO-04-352NI.

GAO Contacts and Acknowledgments

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. For further information about this testimony, please contact me at 202-512-8777 or at stanar@gao.gov. Debra Sebastian, Assistant Director; Chan-My J. Battcher; Lisa L. Berardi; Wayne A. Ekblad; and Jessica A. Evans made key contributions to this report. Additional assistance was provided by Frances Cook, Kathryn E. Godfrey, Nancy A. Hess, Arthur L. James, Jr., Stanley J. Kostyla, and Vanessa R. Taylor.

Appendix I: Scope and Methodology

To address each of our objectives, we met with U.S. Customs and Border Protection (CBP) officials in headquarters and six seaports including, Baltimore, Charleston, Los Angeles-Long Beach, Miami, New York-Newark, and Savannah. These seaports were selected based on the number of cargo containers arriving at the seaport and their geographic dispersion as reported by the U.S. Department of Transportation. At these locations, we also observed targeting and inspection operations. Because we did not select a random, probability sample of ports to visit, the results from these visits cannot be generalized to ports nationwide. We also spoke with CBP's contractor responsible for conducting CBP's peer review and longshoremen's union representatives.

To evaluate how CBP provides assurance that the Automated Targeting System (ATS) targets the highest-risk oceangoing cargo containers for inspection, we reviewed CBP documentation and prior GAO work on performance measures. Additionally, we reviewed CBP's peer review report. To gain an understanding of CBP's random sampling program, we met with CBP officials responsible for this program and reviewed and analyzed CBP documentation, including procedures for examining the randomly selected shipments and documenting the results of the inspections completed for those shipments. We did not independently validate the reliability of CBP's targeting results.

To assess how CBP adjusts ATS to respond to findings that occur during the course of its operational activities, we met with CBP officials responsible for gathering and disseminating intelligence and for incorporating intelligence into CBP's targeting operations. Further, we reviewed CBP policies and procedures on intelligence gathering and disseminating as well as intelligence received and resulting changes to ATS rules and weights. We did not assess the quality of intelligence received or the appropriateness of adjusted rules and weights. To determine how targeting officers' feedback and inspection results are used to adjust ATS rules and weights, we met with CBP officials responsible for collecting and maintaining data on suggestions provided by targeting officers and reviewed CBP data on the suggestions received over a 7 month period. Regarding inspection results, we reviewed CBP's policies and procedures for documenting inspection results. Additionally, we reviewed CBP's manuals identifying the specific details of an inspection completed and observed officers entering inspection results into the ATS findings module during our site visits. Further, during these visits, we discussed how CBP offices at the seaports may use inspection results to enhance their targeting efforts. Last, we met with CBP officials and reviewed CBP documentation on its current and planned findings module.

To determine the status of recommendations from GAO's February 2004 report to (1) establish a testing and certification process for CBP staff who complete the national targeting training to provide assurance that they have sufficient expertise to perform targeting work and (2) work with longshoremen's unions to address fully their safety concerns so that the noninstrusive inspection equipment can be used to conduct inspections efficiently and safely, we reviewed and analyzed data on the number of officers trained and certified in sea cargo targeting. We also reviewed CBP's Sea Cargo Training Manual as well as CBP evaluations assessing the quality of its Sea Cargo Training course. We did not assess the quality of this training. Regarding longshoremen's union concerns, we reviewed scientific literature related to radiation safety and the Nuclear Regulatory Commission guidelines on radiation levels. We also spoke with longshoremen's representatives to discuss whether CBP had addressed their concerns since we issued our 2004 report. Last, we also met with CBP's Radiation Safety Officer to gain a further understanding of the potential risks associated with CBP's inspection equipment and actions he took to address longshoremen's concerns. We did not assess the appropriateness of radiation safety levels used by CBP.

We conducted our work from October 2005 through March 2006 in accordance with generally accepted government auditing standards.

1700 N. Moore Street, Suite 2250, Arlington, VA 22209
Phone: 703-841-2300 Fax: 703-841-1184
Email: info@retail-leaders.org www.retail-leaders.org

Written Statement for the Record of

The Retail Industry Leaders Association

Submitted for the

Senate Committee on Homeland Security and Governmental Affairs

Permanent Subcommittee on Investigations

Hearing on

Securing the Global Supply Chain

March 30, 2006

On behalf of the Retail Industry Leaders Association (RILA), we welcome the opportunity to submit written comments for the record for this important hearing on securing the global supply chain.

The Retail Industry Leaders Association (RILA) is a trade association of the largest and fastest growing companies in the retail industry. Its member companies include more than 400 retailers, product manufacturers, and service suppliers, which together account for more than $1.4 trillion in annual sales. RILA members operate more than 100,000 stores, manufacturing facilities and distribution centers, have facilities in all 50 states, and provide millions of jobs domestically and worldwide.

RILA members share the common goal of all Americans of making the global supply chain safe and ensuring that the movement of cargo through the global supply chain is as secure as possible. As the largest users in the global maritime supply chain, we have an enormous stake in cargo security and are committed to helping the government further enhance security throughout the system. While a great deal has been accomplished to improve supply chain security since the tragic events of September 11, 2001, the government and private sector stakeholders must continue to work together to improve security.

We strongly believe that security legislation, regulations, and public-private partnerships can achieve the dual objectives of enhancing security while continuing to facilitate legitimate global commerce. We urge Congress to avoid "feel good" measures that have a very limited effect on enhancing security but that actually further impede the flow of legitimate commerce and create a false sense of security. A primary goal of those who would disrupt the supply chain is to damage the U.S. economy by any means possible. If commerce is disrupted in a way that damages the ability of Americans to hold well-paying jobs, provide for their families, and generate economic growth that helps the entire world, then the terrorists have achieved a key goal.

Supply chain security is a global issue that cannot be addressed unilaterally. The most effective supply chain security measures are those that push our borders out, assessing vulnerabilities and identifying threats to cargo shipments before they reach U.S. ports. Effective cargo security requires a multi-layered, unified approach that must be international in scope. While recent policy debates have focused on who owns assets in the supply chain system, nobody should dispute that it is better to detect or disarm weapons or contraband thousands of miles from our shores than after their arrival in the U.S.

RILA and its members have played a critical leadership role in shaping supply chain security efforts. From requiring new security language in contracts with their business partners to testing new technologies and ways to identify container tampering, it is private sector stakeholders that have been the innovators in securing their supply chains to protect their employees, customers and businesses. Congress should allow the private sector, working closely with the Department of Homeland Security and other government and non-government interests, to continue to test and deploy the systems and technologies that prove most effective. No one has a greater interest in security than the private sector companies who depend on a secure and efficient supply chain for the safety of their employees and customers and efficient operations of their businesses.

Current Initiatives

As members of the committee are aware, a number of regulations and initiatives have already been undertaken to protect the U.S. from a terrorist attack affecting the supply chain, but we must continue to identify and address vulnerabilities. RILA members have supported a number of important initiatives, such as the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the 24-Hour Rule, the Bioterrorism Act, the Maritime Transportation Security Act (MTSA) and the International Ship and Port Facility Security Code (ISPS). Each of these regulations and initiatives address different aspects of supply chain security. The Committee's investigation and that of the Government Accountability Office will help the Department of Homeland Security, U.S. Customs and Border Protection and U.S. Coast Guard and other agencies continue to improve these programs.

There is still a great deal of work that needs to be done on supply chain security. RILA believes that there are several issues that Congress should consider as it moves forward with initiatives to secure the global supply chain.

Continuing Areas of Work
Container Screening

RILA supports 100% *screening* of containers, but a policy requiring 100% physical inspection of containers is neither effective as a deterrent nor feasible operationally as a security enhancement measure. Rather than enhancing security, setting an arbitrary number of physical inspections of containers would result in commerce grinding to a halt, in effect creating much of the same harm to the nation's and the world's economy that a terrorist incident would cause. Inspections are most effective when focused on areas of risk. U.S. Customs and Border Protection (CBP) should continue to focus on identifying high-risk cargo and physically inspecting 100% of the cargo that is deemed high risk by the National Targeting Center.

CBP receives detailed information about every single container coming into the U.S. prior to that container being loaded at a foreign port and has developed elaborate mechanisms to utilize intelligence and other risk factors to differentiate the true "needle in the haystack" from the overwhelming percentage of cargo containers that present no security risk. Again, setting arbitrary and mandatory percentages of cargo that must be physically inspected will do nothing to enhance security and would be contrary to the mission of the effective risk management system DHS already has in place.

RILA is committed to improving cargo container screening by identifying additional cargo data that can help with the identification of high-risk cargo. The Department of Homeland Security should work with cargo owners and others who own supply chain information to determine what data elements are needed for security risk assessment, who has the information, when the information can be submitted, how it will be used and, most importantly, how it will be protected.

However, even as DHS works to improve its risk assessment efforts, RILA supports efforts to ensure that we have a "zero tolerance" policy for nuclear and radiological material entering our country. While it is preferable to have that screening done overseas as occurs at CSI ports covering the great majority of cargo bound for the U.S., so long as we allow smaller ports

to ship to the U.S., we will need a robust detection regime at our domestic ports as well. Thus it should be the highest priority for CBP and DHS to ensure that those ports participating in the Container Security Initiative have the best technology available to detect radiation and that domestic ports achieve universal nuclear and radiological detection capability. Recent Government Accountability Office (GAO) reports have identified weaknesses in both aspects of the nuclear and radiological detection regime, and RILA supports the work of the Domestic Nuclear Detection Office to build this most critical layer of our defenses.

In addition to the deployment of the Radiation Portal Monitors at U.S. ports, RILA also encourages DHS and CBP to consider other models to help conduct container screening overseas. One such model, which has received a great deal of attention, is the Integrated Container Inspection System (ICIS), which is currently being tested at two terminals in Hong Kong. While we, along with CBP, believe that this model fits with the multi-layered approach, there are still many questions and operations issues that need to be discussed and worked out before such a system is implemented. We strongly urge DHS and CBP to continue to work with the private sector on ICIS and other models to successfully address the operational issues.

The recent GAO report also underscores the need to keep in mind that technology is only one part of the overall solution. Members of Congress must remember that there is no technological "silver bullet" for supply chain security. RILA encourages appropriate testing of all proposed technology solutions to determine which have the greatest reliability before being adopted by the government and industry. Security must be built into the global supply chain from origin to delivery, leveraging the best of current and emerging technologies. It is important that promising technologies be developed by dedicating adequate funds to R & D. At the same time, we must be wary of adopting technological solutions that merely create a false sense of security – too much is at stake to put our trust behind cosmetic, "feel good" security measures. Rushing unproven and/or faulty technology into supply chain security without thorough implementation testing solely for the sake of doing something about security will undermine progress made to date, contribute to a false sense of security and in the end, prove to be a costly ineffective security measure.

Successful security will require a continuation of the multilayered approach that DHS has been following. Congress should outline policies and goals and let DHS find the smartest and most effective way to meet those goals. DHS must retain the flexibility to consider a variety of new technologies rather than being forced into deploying unproven "gadgets". Before any technology can be mandated, DHS must ensure the technology's functionality and application as well as work with the trade community to determine the best methods to deploy them in order to achieve maximum results.

TWIC

In keeping with increasing security at U.S. ports, RILA also endorses prompt implementation of the Transportation Workers Identification Credential (TWIC), a standardized ID containing biometric information that vets the identity and background of the cardholder. All individuals with access to cargo and secure areas of our nation's ports would carry the TWIC, and its potential for use extends to workers throughout our nation's critical infrastructure systems.

Continuity Planning

RILA members also believe that more attention needs to be paid to continuity planning and restoration of trade. In the event of an incident of national significance at a port caused by terrorism or natural disaster, there needs to be a well-coordinated response not only between federal government agencies, but also those at the state and local levels to ensure that commerce continues to move throughout the supply chain. Should an incident occur, everyone must be on the same page as to how to respond. In addition, Congress and the Administration need to ensure that the various agencies involved in homeland security do not duplicate ongoing efforts.

For example, if an incident were to occur in the Port of Los Angeles, that port as well as the Port of Long Beach might have to be shut down during the incident investigation and response. What would happen to other ports on the West Coast? Would Seattle/Tacoma remain open? Would incoming cargo be able to be diverted to other ports? While individual ports have worked on contingency plans for their own facilities, have there been discussions among ports geographically located near each other as to how they would work together? Will all maritime vessels be required to stop where they are or will vessels at non-incident ports be allowed to continue to move?

It is not clear to the business community at this time as to who will be making these critical decisions. This vital information is needed by the trade community to plan appropriately. While certain details cannot be shared because of security concerns, RILA believes that a central communication point or channel must be established so that communications can be streamlined. DHS has begun to work on this with the release of the Maritime Incident Response Plan, which is one of the supporting elements to the National Strategy on Maritime Security, but more work needs to be done. One needs only to look at the experience of Hurricane Katrina to understand the need to have a well-coordinated response that ensures commerce will continue to flow through our nations' ports in the wake of an incident.

Likewise, each country has an interest in ensuring that the global supply chain is kept safe. A major terrorist incident in the U.S. will not impact just one port or one city or even one country. The impact will be felt around the globe. Careful planning and cooperation among governments is important, and government's active collaboration with the private sector is extremely critical. Supply chain security is simply too complicated for the public sector to act effectively without partnering with private industry.

Conclusion

We thank the Senate Permanent Subcommittee on Investigations for the opportunity to submit written testimony for the record. We applaud the subcommittee's reports and hearings on supply chain security and congratulate Chairman Coleman, Ranking Member Levin, Full Committee Chairwoman Collins, Full Committee Ranking Member Lieberman and their staffs for focusing attention on these key issues. RILA strongly believes that government, industry and other stakeholders need to maintain an ongoing, robust dialogue on how best to strengthen port

and supply chain security, rather than allowing the debate to intensify and recede as dictated by external factors.

RILA and its members stand ready to continue to work with both Congress and the Administration on improving the security of U.S. ports and the global supply chain. If you have any questions, please contact Jonathan Gold, Vice President Global Supply Chain Policy, or Paul T. Kelly, Senior Vice President, Federal and State Government Affairs.

# # #

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

April 24, 2006

OFFICE OF THE ADMINISTRATOR

The Honorable Norm Coleman
Chairman
Permanent Subcommittee on Investigations
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

In accordance with section 720 of Title 31, United States Code, I am writing to provide my Management Decision on the Government Accountability Office (GAO) report GAO-06-311, *COMBATING NUCLEAR SMUGGLING: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries*. The GAO was requested by the Senate Homeland Security and Governmental Affairs Committee, Permanent Subcommittee on Investigations to examine the (1) progress U.S. programs have made in providing radiation detection equipment to foreign governments, including the current and expected costs of these programs; (2) challenges U.S. programs face in this effort; and (3) steps being taken to coordinate U.S. efforts to combat nuclear smuggling in other countries.

GAO's review found that U.S. efforts to install and effectively operate radiation detection equipment in other countries face a number of challenges including: corruption of some foreign border security officials, technical limitations of some radiation detection equipment, inadequate maintenance of some equipment, and the lack of supporting infrastructure at some border sites.

NNSA generally agrees with the report and the recommendations. The main issues raised in the report – combating corruption and upgrading older equipment – are long-time priorities for the Second Line of Defense Program. The Second Line of Defense Program is structured to fully address each of these issues.

Enclosed is my Management Decision to the recommendations contained in GAO's report.

An original letter was sent to the Ranking Minority Member.

If you have any further questions, please contact me or C. Anson Franklin, Director, Office of Congressional, Intergovernmental and Public Affairs, at 202-586-8343.

Sincerely,

Linton F. Brooks
Administrator

Enclosure

NNSA's MANAGEMENT DECISION
GAO Report, GAO-06-311, Issued 3/14/2006
COMBATING NUCLEAR SMUGGLING: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries

To strengthen program management and effectiveness, we recommend that the Secretary of Energy, working with the Administrator of the National Nuclear Security Administration, take the following two actions:

Recommendation 1

Integrate projected spending on specific anticorruption measures into the long-term cost estimates for the Second Line of Defense-Core program.

Management Decision

Concur

NNSA has accomplished a significant portion of this work. We will factor cost estimates for centralized communications systems and personnel reliability programs. Since this is an ongoing effort, we believe that NNSA has met the intent of the recommendation.

Recommendation 2

Upgrade less sophisticated portal monitors previously installed by other U.S. agencies where DOE has determined this to be appropriate as soon as possible and include funding to accomplish this in DOE's planning and budgeting process.

Management Decision

Concur

NNSA's plans and programs to upgrade these monitors in full-site installations as part of a country-wide program are captured within NNSA's Planning, Programming, Budgeting and Evaluation process. As such, the funding has been requested to accelerate this process. NNSA believes that we are responsive to the recommendation and have met its intent.

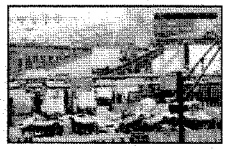
Inspectors: Security lags when traffic jams

SPECIAL REPORT: Bridge operator pushes to keep border travel moving. Government officials deny cutting corners.

BY TAMARA AUDI
FREE PRESS STAFF WRITER

March 29, 2006

On a weekend night earlier this month, 12 big rigs from Detroit were lined up on the Canadian side of the Ambassador Bridge, waiting to be searched by inspectors who were on the lookout for a produce truck thought to be carrying drugs.



Traffic crosses the Ambassador Bridge earlier this month. Amid heightened terror concerns, about 9.4 million vehicles crossed the bridge in 2005, bridge officials said. (Kathleen Galligan/Detroit Free Press)

But before the Canadians could scan the trucks, their supervisor received a call from the U.S. company that owns the bridge. The trucks were snarling traffic. And the bridge's owner wanted traffic cleared quickly, an inspector working that night said.

What happened next, according to customs inspectors and security experts, is what routinely happens on the U.S.-Canadian border when security clashes with commerce: Commerce wins.

"We stopped the inspection," a Canadian inspector said, and let the trucks pass.

Despite fears of terrorism and other security concerns at U.S. ports and border crossings since Sept. 11, 2001, U.S. and Canadian inspectors on the Ambassador Bridge and elsewhere say they are routinely told by supervisors to wave vehicles through checkpoints without scrutiny to satisfy commercial interests.

Though government officials in the United States and Canada deny safety is compromised, inspectors say security lapses are a particular problem at the Ambassador Bridge -- the busiest northern border crossing, and one of only two along the U.S.-Canadian border that are privately owned.

In one practice known as lane flushing, inspectors at the bridge -- owned by the Detroit International Bridge Co. -- say supervisors force them to wave through long lines of cars and trucks to ease congestion, without asking even cursory questions of drivers or passengers.

"When the traffic backs up to a certain point, you know the call is going to come" from the bridge company, one bridge inspector told the Free Press. "Then management jumps like lapdogs."

Robert Perez, port director of Detroit for U.S. Customs and Border Protection, an agency of the Department of Homeland Security, denied lane flushing takes place. Perez said his office tries to cooperate with bridge and tunnel operators, and that inspectors might view that cooperation as caving in to commercial interests.

"The people in the community, both in Detroit and Windsor, should feel good about the fact that their border crossings are safer than ever before," Perez said.

The Free Press interviewed more than a dozen inspectors, former inspectors, Homeland Security officials, customs supervisors, politicians and border security experts -- including six inspectors assigned to the Detroit-Windsor border. All but one of the inspectors -- a Canadian union leader -- spoke on condition of anonymity, noting agency restrictions on media interviews and saying they feared job reprisals if named.

The allegations come as U.S. border security has faced its closest scrutiny since the 2001 terrorist attacks.

Congressional opposition recently scuttled a plan to have a Dubai-owned firm manage six U.S. ports. And Tuesday, as Congress debated tougher border security as part of an immigration package, a Senate subcommittee was investigating how undercover agents drove into the United States from Canada and Mexico with nuclear material.

Technology touted

U.S. and Canadian customs officials, and representatives from the bridge company -- owned by trucking magnate Manuel (Matty) Moroun -- insist security is never compromised for commerce and say, in fact, the reverse is true: Better technology, improved facilities and better cooperation between business and government make the border more secure and efficient.

Perez noted that the bridge and Detroit-Windsor Tunnel now feature high-tech surveillance -- invisible to travelers -- such as radiation detectors and electronic prescreening programs. And customs agents in Detroit seized more than 5,000 pounds of drugs last year, an eightfold increase over the previous year, he said.

Dan Stamper, president of the bridge company, said it has spent millions to expand facilities since 9/11 and would never ask inspectors to "give up any of their security initiatives to move traffic faster."

Bridge inspectors concede that, even under the best of circumstances, they could not fully inspect every vehicle entering the United States without crippling trade. Thus, they say, it is not unusual for drivers to pass inspection with only a few questions asked.

What they object to, they say, are orders from supervisors to wave through long lines of cars and trucks with no questioning at all. Sometimes, inspectors say, they have been told to stop inspecting a particular vehicle to open more booths when traffic backs up.

"They call and say, 'You're holding us up too much.' And they always win that argument," said Charles Showalter, national president of one of the two unions representing U.S. Customs and Border Protection officers. He said when inspectors or the union object, Homeland Security officials "call it 'acceptable risk.' It's 'Hurry up, hurry up, hurry up, hurry up.' Nobody wants to slow down commerce."

Bridge inspectors say this can happen once a week or more at the Ambassador Bridge -- one of two privately owned crossings on the U.S.-Canadian border. The other is a bridge in International

Falls, Minn. However, they also say that inspectors are also pressured to speed traffic at government-owned crossings that are run by private companies.

The Detroit-Windsor Tunnel, for example, is run by a private company but owned by the City of Detroit on one side and Windsor on the other. Toll profits are shared with the cities.

Tolls collected at the Ambassador Bridge go to the bridge company, owned by Moroun of Grosse Pointe Shores.

Keeping the wait down

Since 9/11, traffic has declined about 30% at Detroit's border crossings.

To counter memories of long delays in the months after Sept. 11, the Detroit-Windsor Tunnel tries to keep waits under 20 minutes. Both the tunnel and bridge post wait times on their Web sites. During rush hour on an evening this week, bridge travel to and from Canada was under 15 minutes. The tunnel wait was under 6 minutes.

Neal Belitsky, executive vice president of the Detroit & Canada Tunnel Corp., which operates the tunnel, said he considers a 20-minute wait as "the outer limits for acceptability" for the roughly 29,000 vehicles that pass through daily.

"When we see traffic getting to that threshold, we will start calling customs and saying we need more lanes," he said. "That's a standard part of the business and we all do it."

He added there are times when customs denies his request and he backs off.

Danny Yen, spokesman for the Canadian Border Services Agency in Windsor, said, "We've had our challenges" with the bridge company, but "we never compromise security for trade. It's a balance."

Haste makes risk, some say

But inspectors say the rush to speed traffic has spawned practices -- such as lane flushing -- that put security at risk.

"Lane flushing happens all over the place, at every crossing," Showalter said. "The traffic backs up. The supervisor gets a call" from private border businesses. "They run an officer with a canine through the line of cars, and the officers on the primary inspection lanes are told not to ask questions."

About 9.4 million vehicles crossed the Ambassador in 2005, according to bridge officials. Collectively, the bridge, tunnel and a commercial train tunnel account for nearly a quarter of all U.S. trade with Canada, the bulk of it by trucks crossing the bridge. When trade is delayed at the border, Michigan's automobile-reliant economy suffers most, a recent Ontario Chamber of Commerce study shows. Automakers use a "just-in-time" delivery system that depends on parts crossing promptly. A delay of even a few hours can cost millions.

A difficult balance

Perez, the Detroit port director, said changes intended to balance trade and security issues mean that some vehicles don't have to be checked as frequently. The government's so-called trusted traveler programs, for instance, allow prescreened businesses to cross faster and with fewer inspections, though critics say terrorists could exploit such efforts.

Colleen Kelley, president of the National Treasury Employees Union, a union representing 150,000 federal workers, including inspectors, said that pressure to speed trade means "something's got to give." What usually gives, she said, is thorough inspection work.

"The balance of trade and security became a battle that we really lost to trade years ago," said Joseph King, a professor and terrorism expert at John Jay College of Criminal Justice in New York who worked for U.S. Customs for 37 years. "Customs has become an honor system where the industry controls it, and periodically the government comes in and monitors."

And yet, ask Moroun -- whose company gets a reported $60 million annually in bridge revenue and spent $645,000 on lobbying and consulting over the past nine years -- about inspectors and he says, "They're very independent."

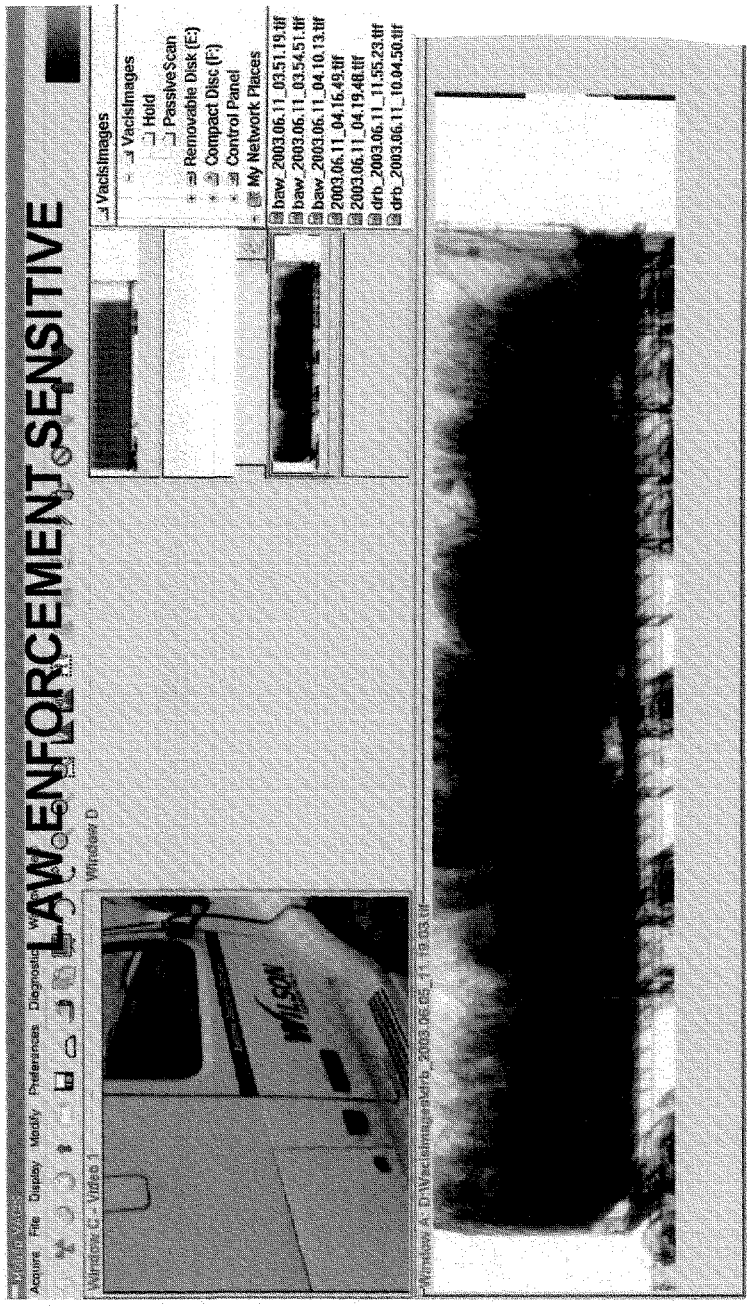
On the other side of the river, Marie-Claire Coupal, a Canadian customs inspector and local union leader, said she doesn't feel very independent lately. Of Moroun, she says, "He calls the shots around here."

The bridge company's Stamper responds that his firm has a duty to keep trade moving. And he notes that a recent study rated the Ambassador's travel times "clearly superior" to six other crossings.

Sept. 11, Stamper said, was a wake-up call for him, too. After the attacks, heightened security led to 14-hour bridge delays. Choking the economy was, after all, a major goal of the terrorists, he said.

So the main threat Stamper sees is not a dirty bomb, or suicide bombers. "Our biggest threat is our own government's reaction to the border."

###



Permanent Subcommittee on Investigations
EXHIBIT #15

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Audit of Screening Trucks Carrying Canadian Municipal Solid Waste

(Unclassified Summary)

Office of Audits

OIG-06-21

January 2006

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our DHS oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report presents a public summary of our limited official use report assessing the Bureau of Customs and Border Protection's process for screening trucks carrying Canadian municipal solid waste. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendation contained in this report has been developed according to the best knowledge available to our office, and has been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

UNCLASSIFIED SUMMARY

The greater Toronto, Canada area has been shipping municipal solid waste (MSW) to Michigan landfills for disposal since 1998. During calendar year 2004, Michigan landfills received approximately 100,000 truckloads of Canadian MSW, an 8 percent increase over calendar year 2003. Another 10,000 shipments of MSW enter the U.S. through 9 other ports of entry (POE) that accept Canadian and Mexican MSW. Over the past two years, trucks carrying Canadian MSW were found to contain medical waste, illegal drugs, and illegal currency. At the request of Senators Levin and Stabenow and Representative Dingell, our office reviewed the effectiveness of the Bureau of Customs and Border Protection's (CBP) screening of trucks carrying Canadian MSW.

CBP has the authority[1] to search all persons, baggage, and merchandise arriving in the U.S. to detect and seize smuggled instruments of terror, and other contraband, such as illegal drugs. CBP carries out its responsibility by using screening equipment and physical inspections. For example, every passenger vehicle and truck entering the U.S. at the Detroit and Port Huron POE pass through a radiation portal monitor (RPM), and selected trucks receive a Vehicle and Cargo Inspection System (VACIS)[2] screening.

Our audit work was conducted at CBP Headquarters in Washington, DC, and at the ports of Detroit and Port Huron, Michigan. We evaluated CBP entry and screening procedures and observed CBP personnel implementing those procedures at Michigan landfills and at the ports of Detroit and Port Huron. We also gathered and analyzed information regarding techniques for screening MSW from other northern and southern border ports. In addition, we made site visits to three MSW transfer stations in the greater Toronto area.

Improvements are needed in the inspection process. For example, the ports vary in how they select and inspect cargo and conduct their VACIS examinations. In addition, there is no Centralized Examination Station in Michigan.

We are recommending that the Commissioner of CBP conduct a risk analysis and develop minimum requirements for selecting and inspecting trucks carrying Canadian MSW.

[1] 19 USC § 1467; 19 CFR § 162.6.
[2] A VACIS machine uses gamma rays to produce a visual presentation of a truck's contents. The image is similar to an x-ray.

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

For Official Use Only

Audit of Screening of Trucks Carrying Canadian Municipal Solid Waste

Office of Audits

OIG-06-21

January 2006

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared by our office as part of our DHS oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This review was conducted at the request of Senators Carl Levin, Debbie Stabenow and Representative John D. Dingell of Michigan. We assessed the Bureau of Customs and Border Protection's process for screening and inspecting trucks carrying Canadian municipal solid waste into the United States. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents

Appendices

Abbreviations

ATS	Automated Targeting System
CBP	Bureau of Customs and Border Protection
CES	Centralized Examination Station
GAO	Government Accountability Office
MSW	Municipal Solid Waste
OIG	Office of Inspector General
POE	Ports of Entry
PRD	Personal Radiation Device
RIID	Radiation Isotope Identifier Device
RPM	Radiation Portal Monitor
VACIS	Vehicle and Cargo Inspection System
WMD	Weapons of Mass Destruction

OIG

Audit Report

Department of Homeland Security
Office of Inspector General

FOR OFFICIAL USE ONLY

Executive Summary

The greater Toronto, Canada area has been shipping municipal solid waste (MSW) to Michigan landfills for disposal since 1998. During calendar year 2004, Michigan landfills received approximately 100,000 truckloads of Canadian MSW, an 8% increase over calendar year 2003. Another 10,000 shipments of MSW enter the U.S. through 9 other ports of entry (POE) that accept Canadian and Mexican MSW. Over the past two years, trucks carrying Canadian MSW were found to contain medical waste, illegal drugs, and illegal currency. At the request of Senators Levin and Stabenow and Representative Dingell, our office reviewed the effectiveness of the Bureau of Customs and Border Protection's (CBP) screening of trucks carrying Canadian MSW.[1]

Our audit work was conducted at CBP Headquarters in Washington, DC, and at the ports of Detroit and Port Huron, Michigan. We evaluated CBP entry and screening procedures and observed CBP personnel implementing those procedures at Michigan landfills and at the ports of Detroit and Port Huron. We also gathered and analyzed information regarding techniques for screening MSW from other northern and southern border ports. In addition, we made site visits to three MSW transfer stations in the greater Toronto area. The audit objective, scope, and methodology are discussed in more detail in Appendix A of this report.

CBP has the authority[2] to search all persons, baggage, and merchandise arriving in the U.S. to detect and seize smuggled instruments of terror, and other contraband, such as illegal drugs. CBP carries out its responsibility by using screening equipment and physical inspections. For example, every passenger vehicle and truck entering the U.S. at the Detroit and Port Huron POE pass through a radiation portal monitor (RPM) and selected trucks receive a Vehicle and Cargo Inspection

[1] The request letter is included as Appendix B.
[2] 19 USC § 1467; 19 CFR § 162.6.

System (VACIS)[3] screening. During special operation days, the contents of selected trucks are physically inspected. However, because of the limitations of the screening equipment,[4] the large number of MSW trucks crossing POE, the limited resources available for conducting time-intensive inspections of MSW, and the difficulty in conducting physical inspections of MSW, the likelihood of finding prohibited items is minimal.

We are recommending that the Commissioner of CBP conduct a risk analysis and develop procedures and minimum requirements for selecting and inspecting trucks carrying Canadian MSW.

Background

According to Title 19 Code of Federal Regulations, Section 162.6, all persons, baggage, and merchandise arriving in the customs territory of the U.S. from places outside thereof are liable to inspection and search by a customs officer.

Over 99% of Canadian MSW coming into Michigan flows through two major POE, the Blue Water Bridge in Port Huron and the Ambassador Bridge in Detroit. During calendar year 2004, these POE accepted approximately 100,000 shipments of MSW for Michigan landfills, an increase from approximately 92,600 during calendar year 2003. The majority of the shipments are from the greater Toronto area. MSW from other areas of Canada and Mexico enter the U.S. through an additional nine POE that processed approximately 10,000 trucks in calendar year 2004.

[3] A VACIS machine uses gamma rays to produce a visual presentation of a truck's contents. The image is similar to an x-ray.

[4] We have reported on the limitations of RPM and VACIS equipment in DHS OIG report number OIG-04-040, September 2004.

Table 1 shows the number of MSW trucks entering the U.S. during calendar year 2004.

Table 1
MSW Truck Entering U.S. Ports
Calendar Year 2004

Ports	Number of Shipments	Percentage
Port Huron, Michigan	90,174	82.1
Detroit, Michigan	9,250	8.4
Buffalo, New York	7,580	6.9
Sumas, Washington	2,252	2.1
Sault Ste. Marie, Michigan	534	0.5
San Luis, Arizona	38	0
Other Ports	19	0

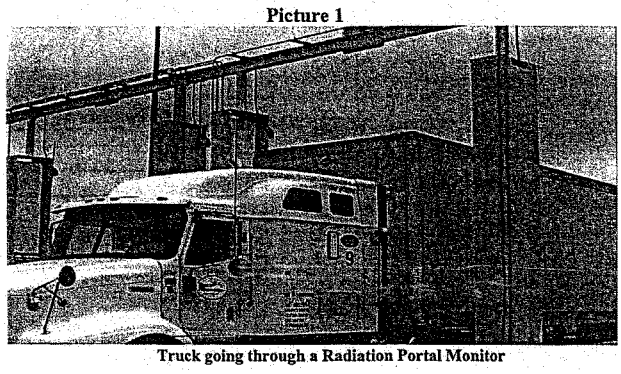
In Toronto, the MSW is unloaded from garbage trucks and reloaded onto larger long-distance tractor-trailers for shipment to Michigan landfills. At some of the transfer stations, the loaded trucks are driven through an RPM prior to departure to the U.S.

CBP Inspections

At the Detroit and Port Huron POE, every passenger vehicle and truck must pass through an RPM. An RPM is a non-intrusive tool that screens vehicles for nuclear and radiological materials.

Picture 1 shows an MSW truck passing through a RPM.

Picture 1



Truck going through a Radiation Portal Monitor

If an RPM or a Personal Radiation Detector (PRD)[5] alerts to the presence of radiation, the MSW truck receives a second screening using a different RPM. If the second RPM also alarms, the truck undergoes secondary examination. The secondary examination would involve CBP officers using a Radiation Isotope Identifier Device (RIID) to identify the source of the radiation (specific isotope). The truck may also undergo a VACIS examination. The secondary examination generally involves a physical examination of the vehicle. CBP does not have the capability to unload and inspect the contents of a MSW truck at the POE. Once the source of the specific radiation is determined, the vehicle will be released into the U.S., or processed for immediate return to Canada.[6] If a violation has occurred, a penalty might be issued. In September 2004 we reported on the limitations of RPM, VACIS, PRD, and RIID equipment in report number OIG-04-040.

[5] The PRD is a small, self-contained personal safety device used for detecting radiation.
[6] Radiation can be present in many commonly used materials such as cat litter and clay tiles.

Special Operations

In July 2003, CBP initiated special operation days called "Dump in Detroit" and "Screen Waste in Port Huron" to determine if trucks hauling MSW into the U.S. are in compliance with import laws and regulations. During the special operations, trucks are selected after they have gone through the RPM. All trucks entering the U.S. at the ports of Detroit and Port Huron drive through an RPM. Trucks cannot be selected for special operations until they have gone through the RPM. The truck driver's entry documents are also reviewed to see if the driver has any outstanding warrants or legal issues in the U.S. or Canada. After the documents are confirmed, the truck is escorted to a landfill for a more thorough examination of its contents. Before the trucks are escorted to the landfill, a canine, if available, will be used to inspect the trucks. Since the special operations began, 629 trucks have been inspected, including 552 at the port of Detroit and 77 at Port Huron.

Results of Audit

Vulnerabilities in Screening Equipment and Physical Inspections

CBP does not have an effective method to screen and inspect the 350 truckloads of MSW that enter the U.S. daily through the Detroit and Port Huron POE. The effectiveness of RPMs and other equipment used to test for the presence of radiation is limited. VACIS visual presentations cannot easily distinguish drugs, weapons, or other contraband in MSW. In addition, physical inspections are of limited value because it is difficult to thoroughly inspect compacted MSW to identify illegal cargo, and relatively few inspections are performed because they are labor intensive. Further, physical inspections of the cab and the tractor are not routinely performed.

RPM and VACIS Examinations

The effectiveness of RPM and VACIS examinations is limited. In a September 2004 classified report, we identified needed improvements in the application of RPM technology. In addition, the effectiveness of the VACIS imaging system is limited by the nature of MSW. Because MSW is dense when compacted for transportation and is not a

homogenous product, it can be difficult for the officers to identify anomalies in the visual representation. Other commodities present a clearer and more uniform image. However, the imaging system has been useful in detecting some illegal drug smuggling. In one instance, an anomaly in the visual representation was found to be 1,900 pounds of marijuana packed in sports equipment bags. The bags were found in the back of a MSW truck.

The VACIS imaging equipment also has mechanical limitations. At the ports we visited, the truck housing the equipment and the VACIS equipment itself were often out of service due to mechanical problems. The VACIS truck must be driven to a contractor or wait for a technician for repairs. Also, the equipment is often inoperable in inclement weather (electrical, wind, and snow storms).

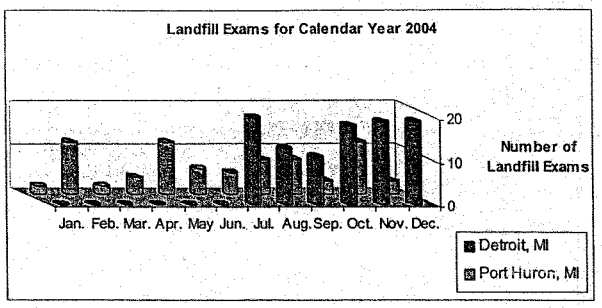
CBP Inspections of MSW

Very few trucks received inspections other than an RPM. All MSW inspections during calendar year 2004 took place under special operation days called "Dump in Detroit" and "Screen Waste in Port Huron." Although the Detroit and Port Huron POE accept 99% of MSW entering Michigan and over 90% of all MSW entering the U.S., the contents of less than 2/10 of 1% of MSW trucks are selected for physical inspections.

During calendar year 2004, 77 of the 90,174 MSW trucks that came through Port Huron were selected for landfill inspections. At the port of Detroit, 100 of 9,250 MSW trucks were selected for inspection. However, all inspections at Detroit occurred during July through December; no inspections were performed during January to June. CBP personnel told us they did not perform any landfill examinations during the latter period because officers were assigned to higher risk priorities.

Table 2 shows the number of landfill examinations performed by month during 2004 for the Port Huron and Detroit POE.

Table 2



Poor weather conditions, difficulty getting into landfills, distances to the landfills, the length of time required to escort MSW trucks to a landfill and conduct an inspection, limit the number of landfill exams conducted by CBP. The Michigan landfills are located from 25 to 90 miles from the POE. Three officers and a supervisor conduct landfill examinations either on overtime or on regular hours, with their normal work assignments performed on an overtime basis. CBP officers typically select no more than five trucks to accompany to the landfill, observe the unloading, and examine the contents. The officers then return to the POE. The process from selection to release of the trucks after the examination, can take from 3 to 6 hours.

Physical examinations at landfills are difficult to perform because of unhealthy and dangerous environmental conditions. The presence of blood, medical waste, syringes, and the commingling of household chemical products, can cause skin irritation, respiratory problems, and diseases, such as hepatitis. Officers are also exposed to bird droppings from the multitude of birds that fly above the landfills.

Picture 2

CBP Officers at a Michigan landfill unloading a MSW truck

In addition, the MSW is generally so tightly compacted when a truck is loaded, that it is hard to identify specific items, as they are unloaded at the landfill. There have been fires inside these trucks caused by spontaneous combustion in the tightly compacted MSW.

Further, the landfill surfaces are unstable and slippery during rain, snow, and ice. Officers can be injured climbing through the waste or by other commercial trucks unloading garbage in the same area. Poor weather conditions can also limit the number of landfill exams because of the conditions of the roads and the distances to the landfills.

CBP officials consider inspection activities to be a local decision based on a port officials' assessment of risk, available resources, and workload. CBP officials at the ports of Detroit and Port Huron told us they use local intelligence, officer judgment, random sampling, and targeting scores from CBP's Automated Targeting System (ATS) to select trucks carrying MSW for further examination. CBP officials said they have not conducted a comprehensive assessment of risks facing the northern border.

Centralized Examination Station

Centralized Examination Stations (CES) are facilities located near POE that provide the buildings and equipment needed to unload trucks, examine their cargo, and reload. There are no CES near the Detroit or Port Huron POE. Physical examinations are limited to a peek in the back of truck (if the door is opened too much, it cannot be closed again) or a view of the top of an open-top truck covered by a rollback tarp.

CBP solicited bids for a contractor to provide a preexisting facility or to construct and operate a CES for MSW near the Detroit and Port Huron POE. CBP planned to have contractors operate the facility, including unloading and re-loading the MSW trucks and inspecting the contents. The cost of the examinations, under CBP's plan, would be charged to the importer/exporter or importer's/exporter's agent. CBP officers would be present at the CES to oversee the operation.

CBP received one proposal in response to its request. The proposal was for a CES facility 80 miles from the POE. CBP determined that this was too far from the POE. CBP officials believe a CES would allow CBP to conduct more inspections in a safer environment and reduce the cost of inspections. However, according to CBP officials, there appears to be no interest from the private sector in establishing a CES facility closer to the ports, and as a result, CBP is no longer pursuing the CES.

Operating Procedures

CBP relies on local POE officials to decide when to select and inspect MSW trucks. CBP's procedures for special operation days, for example, do not specify how frequently special operation days should occur or how many trucks should undergo inspection during these operations. Lacking nationwide procedures, local port officials drafted local procedures for screening MSW. This resulted in inconsistent inspections by the CBP officers at the various POE. For example, Port Huron's "Screen Waste" procedures instruct the officers to release the trucks selected for inspections if a bottleneck develops at the bridge, while Detroit's "Dump" procedures do not mention release because of bottlenecks.

In addition, Detroit and Port Huron do not conduct VACIS exams in the same way. Detroit images the entire truck after the driver exits. Port Huron starts to image behind the driver; the driver remains in the cab to drive the truck through the imaging process. Consequently, if there were contraband in the cab, the imaging process would not detect it.

Recommendations

We recommend that the Commissioner of CBP conduct a risk analysis and develop procedures and minimum requirements for selecting and inspecting trucks carrying MSW. The procedures should require inspections throughout the year and physical inspections should not be limited to special operations days.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from CBP. We have included a copy of the comments in their entirety as Appendix C. CBP agreed with the recommendations. Below is a summary of CBP's response to the recommendations and our assessment of the response.

CBP concurred with the recommendation and proposed a three part action plan:

The Office of Field Operations (OFO) will request that the Office of Strategic Trade perform a risk analysis of trucks carrying municipal solid waste into the United States.

OFO will review the risk analysis and develop procedures and requirements for selecting and inspecting trucks carrying Canadian municipal solid waste.

OFO will implement the new selection criteria and inspection procedures.

CBP's proposed corrective action, when fully implemented, will satisfy the recommendation. We requested a copy of the risk analysis and a copy of the selection criteria and inspection procedures.

Objective, Scope, and Methodology

The objective of this audit was to determine the effectiveness of the technologies and methodologies used by CBP to screen MSW. Specifically, we determined whether there were vulnerabilities in the technologies and methodologies that CBP used to screen trucks and drivers hauling MSW from Canada, and whether CBP personnel had established consistent, comprehensive, and clear methodologies for screening MSW. The audit scope covered the period January 2003 through March 2005.

We interviewed CBP Headquarters and port personnel responsible for the program. We reviewed regulations, directives, and other guidance related to the screening and examination of MSW. We reviewed MSW entries and analyzed data files received from port personnel.

We conducted our audit work at CBP Headquarters and at the ports of Detroit and Port Huron, Michigan, where we observed the processing and screening of MSW. We selected the ports of Detroit and Port Huron because they have the largest volume of MSW entries nationwide. We also visited two Michigan landfills and observed how MSW is examined. We visited three MSW transfer stations in the greater Toronto area where MSW is unloaded from collection vehicles and briefly held while it is reloaded onto larger long-distance transport vehicles for shipment to landfills or other treatment or disposal facilities. We also gathered and analyzed information regarding techniques for screening MSW from other northern and southern border ports.

We conducted our audit between June 2004 and March 2005 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards.

Appendix B
Request from Representative Dingell, Senator Stabenow, and Senator Levin

FOR OFFICIAL USE ONLY

Congress of the United States
Washington, DC 20510

October 20, 2003

The Honorable Clark Kent Ervin
Acting Inspector General
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Inspector General Ervin:

We are writing to request that your office begin an investigation into the effectiveness of the Bureau of Customs and Border Protection screening of trucks carrying municipal solid waste (MSW). Since January 2003, the City of Toronto has been shipping all of its MSW to Michigan for disposal. Currently, approximately 125-150 trash trucks from Toronto and 30 trash trucks from other Canadian municipalities travel across the U.S. – Canadian border into Michigan for disposal *each day*. The core question we seek an answer to is whether or not the methodologies and technologies used by the Bureau to screen municipal solid waste are as effective as the methodologies and technologies used by the Bureau to screen other items of commerce entering into the United States by commercial motor vehicle transport.

As you may know, Inward Cargo Manifests for these trash shipments simply read "Municipal Solid Waste." Over the course of the past year, there have been numerous cases where trucks were in fact carrying more than was listed on the manifest. 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. In April of this year, police in Sumpter Township, Michigan, found 50 pounds of marijuana in a trash truck. In that instance, Customs agents told Carleton Farms landfill operators to be on the lookout for contraband such as illegal drugs.

In early August of this year, a trailer carrying MSW was pulled over for being overweight. The policemen on duty, after obtaining consent from the driver and passengers, found a blue duffel bag containing $539,200. On September 24, 2003 Customs 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 packed in 59 plastic bags and hockey equipment duffel bags was one of the biggest drug busts in recent Michigan history. Law enforcement officials value the drug's street value at approximately $9 million. A few days later, on September 30, the Macomb County prosecutor's office secured a warrant against a Canadian waste hauling company for violating Michigan law by dumping medical waste in Michigan landfills.

Appendix B
Request from Representative Dingell, Senator Stabenow, and Senator Levin

FOR OFFICIAL USE ONLY

The aforementioned cases are examples of the system working. However, we are concerned that for each truck found with contraband, many more may be getting through the system.

This is an issue of the utmost importance to the citizens of Michigan, and indeed the safety of our Nation. Therefore, we ask that you begin this investigation as soon as possible. If you have any questions, please do not hesitate to contact us, or have your staff contact Kaye Meier in Senator Levin's office at (202) 224-9110.

Sincerely,

John D. Dingell
Member of Congress
U.S. House of Representatives

Debbie Stabenow
Member of Congress
U.S. Senate

Carl Levin
Member of Congress
U.S. Senate

Appendix C
Management Response To Draft Report

FOR OFFICIAL USE ONLY

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

December 20, 2005

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Acting Director
Office of Policy and Planning

SUBJECT: Response to the Office of Inspector General's Draft Report on the Screening of Trucks Carrying Canadian Municipal Solid Waste

Thank you for providing us with a copy of your draft report entitled "Audit of Screening of Trucks Carrying Canadian Municipal Solid Waste" and the opportunity to discuss the issues in this report. The U.S. Customs and Border Protection (CBP) appreciated the opportunity to work with the auditors in constructing a balanced and accurate document. CBP agrees with the overall substance and findings of the report.

The Office of Inspector General (OIG) recommends that CBP conduct a risk analysis and develop procedures and minimum requirements for selecting and inspecting trucks carrying MSW. The procedures should require inspections throughout the year and physical inspections should not be limited to special operations days.

CBP concurs with the recommendations and proposes a three part action plan:

- **Risk analysis performed by the Office of Strategic Trade** – The Office of Field Operations (OFO) will request that the Office of Strategic Trade perform a risk analysis of trucks carrying municipal solid waste into the United States. The analysis will be focused on providing statistically valid examination rates for each type of examination performed. This analysis will be requested within 120 days. The tentative delivery date is May 1, 2006.

- **Development of procedures by OFO** – OFO will review the risk analysis and develop procedures and requirements for selecting and inspecting trucks carrying Canadian municipal solid waste. The tentative delivery date for this is June 1, 2006.

2

- **Implementation of procedures by the OFO** – OFO will implement the new selection criteria and inspection procedures. Full implementation should be completed by August 1, 2006.

CBP has determined that the information in the audit does warrant protection and we are designating the document as "For Official Use Only (FOUO)." Classification of the report as FOUO is clearly justified because of the sensitive nature of the information contained therein. The entire report should be FOUO because it discusses targeting and exam methodology. Please consider CBP's concerns prior to releasing information that has been determined to be sensitive.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Lynn Richardson at (202) 344-2953.

Major Contributors To This Report

Roberta N. Rickey, Field Office Director
Robert Davis, Audit Manager
Elizabeth Haskett, Auditor-in-Charge
Robert Long, Auditor
Mee Lun Williams, Auditor

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretariat
Acting Commissioner, Customs and Border Protection
Assistant Commissioner for Field Operations
Assistant Secretary, Public Affairs
Assistant Secretary, Policy
Assistant Secretary, Legislative Affairs
CBP Audit Liaison
DHS OIG Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

May 4, 2006

Senator Norm Coleman, Chairman
Senator Carl Levin, Ranking Minority Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Chairman and Senator Levin:

In your April 19, 2006 letter to the Comptroller General, you provided a supplemental question for the record from Senator Akaka. You wrote:

"In your statement you noted that corruption is a pervasive problem within certain foreign border security organizations, and that such corruption could compromise the effectiveness of U.S.-funded radiation detection equipment.

Do you have any indication that these detection technologies, including the smaller highly portable hand-held devices, have fallen into the wrong hands and are now being used to measure the effectiveness of shielding a nuclear or radiological device before a terrorist even attempts a border crossing?"

During the course of our review, we did not find any indication of U.S.-funded equipment falling into "the wrong hands." However, as we note in our report, we did find that the Department of State, in its role as lead interagency coordinator, has not maintained accurate information on the operational status and location of all radiation detection equipment provided by U.S. programs. While DOE, DOD, and State each maintain lists of radiation detection equipment provided to foreign governments by their programs, they do not regularly share such information, and there is no comprehensive list of all equipment provided by U.S. programs. Without such a coordinated master list, program managers at DOE, DOD, and State cannot accurately assess if equipment is operational and being used as intended; determine the equipment needs of countries where they plan to provide assistance; or detect whether an agency has unknowingly supplied duplicative equipment to the same country or site. We recommended that the Department of State account for all U.S.-funded radiation detection equipment provided to foreign governments, especially handheld equipment, by creating, maintaining, and sharing among all agencies a comprehensive list of such assistance. State agreed with our recommendation and is taking steps to implement it.

While the lack of accountability over some U.S.-funded radiation detection equipment, especially hand-held equipment, is troubling, we did not find any evidence of such equipment falling into the wrong hands or being used to measure the effectiveness of shielding a nuclear or radiological device before a terrorist even attempts a border crossing.

Sincerely yours,

Gene Aloise
Director, Natural Resources and Environment
U.S. Government Accountability Office

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
SUBMITTED BY
SENATOR CARL LEVIN
to
THE HONORABLE MICHAEL P. JACKSON
Deputy Secretary
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 30, 2006

1. **The Subcommittee report found that 18% of containers identified by CBP as high risk at CSI ports are not inspected overseas. For example, The Subcommittee report noted that in the port of Tokyo, from February 2005 to February 2006, 477 exams of high risk containers were requested by CSI personnel and 430 exams were conducted by Tokyo officials. Therefore, 10% of the high risk containers requested by CSI personnel were not examined at the Tokyo port.**

   a. **At the hearing, I asked you why all containers identified as high risk are not inspected overseas at CSI ports. You responded that you would provide a more complete answer at a later date to the Subcommittee. Please explain why all containers identified as high risk are not inspected at CSI ports.**

      Response: All containers identified as high-risk by the Customs and Border Protection's (CBP) Automated Targeting System (ATS) are targeted by the Container Security Initiative (CSI). Those that, after research and analysis, are found to still pose a risk for terrorism are forwarded for examination. This research and analysis identifies shipments that have been entered incorrectly, which we call "manifest discrepancies" and shipments that have been incorrectly identified due to system errors, which we label "misfires." Additionally, some shipments identified as high-risk by ATS, such as those in the above example of Japan, are not subsequently examined as a result of specific information provided by the host government. This information detailed background and data regarding the shipment's shipper, exporter, and importer, and in many cases, mitigates the risk with the shipment. In cases where the information does not mitigate the risk, and the shipment was not examined by the host government, the CSI team will place on hold for a "Domestic Exam" on the shipment which will be conducted by CBP at this first U.S. domestic port of unlading.

b. At the hearing, I asked how CBP tracks which high risk containers that are not inspected in a foreign country are inspected in the U.S. You stated that "I'm assuming we could show you the CBP audit trail on these issues." Please provide the Subcommittee with the "audit trail" that demonstrates that all containers identified by CBP as high risk are inspected either overseas or in the U.S.

Response: An "audit trail" regarding high-risk cargo not inspected in a foreign country and requiring an inspection overseas is maintained in the ATS through transaction status switches generated by CBP officers. These statuses are generated when CBP officers mark shipments for review, mark shipments for hold, input hold comments, and input findings. The user IDs and date and time stamps are recorded against these actions. A "domestic exam requested" is a transaction status with a "CSI - for Domestic Exam" as a hold type. CBP officers operating overseas at CSI ports set this hold type when they identify a high-risk container for domestic exam that may not have been examined at the foreign port. This switch is used by ATS to present domestic CBP officers with this shipment transaction workload. CBP officers at U.S. ports use ATS to identify these shipments and place domestic holds on those shipments for domestic examination. *Please see the attached screen shots of the ATS system for an illustration of this process.*

2. On March 30, 2006, the GAO released a report, "Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System." The GAO report found that "CBP has not yet put key controls in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction." Please comment on the GAO's findings.

Response: CBP is making progress on each of the key internal controls identified by GAO. Specifically:

(1) CBP has developed and implemented performance measures related to the targeting of cargo containers. CBP has developed and is currently evaluating and refining a formal methodology in which the performance of ATS rules targeting cargo shipments can be assessed.

(2) CBP has begun to compare the results of its random inspections with its ATS inspection results. CBP is reviewing significant seizure results and critical, positive exam results to validate or adjust targeting rules as appropriate on a case-by-case basis. Also, CBP is reviewing certain Compliance Measurement positive findings and recommending appropriate to ATS rule adjustments, specifically focusing on significant findings (i.e., restricted/prohibited and narcotics).

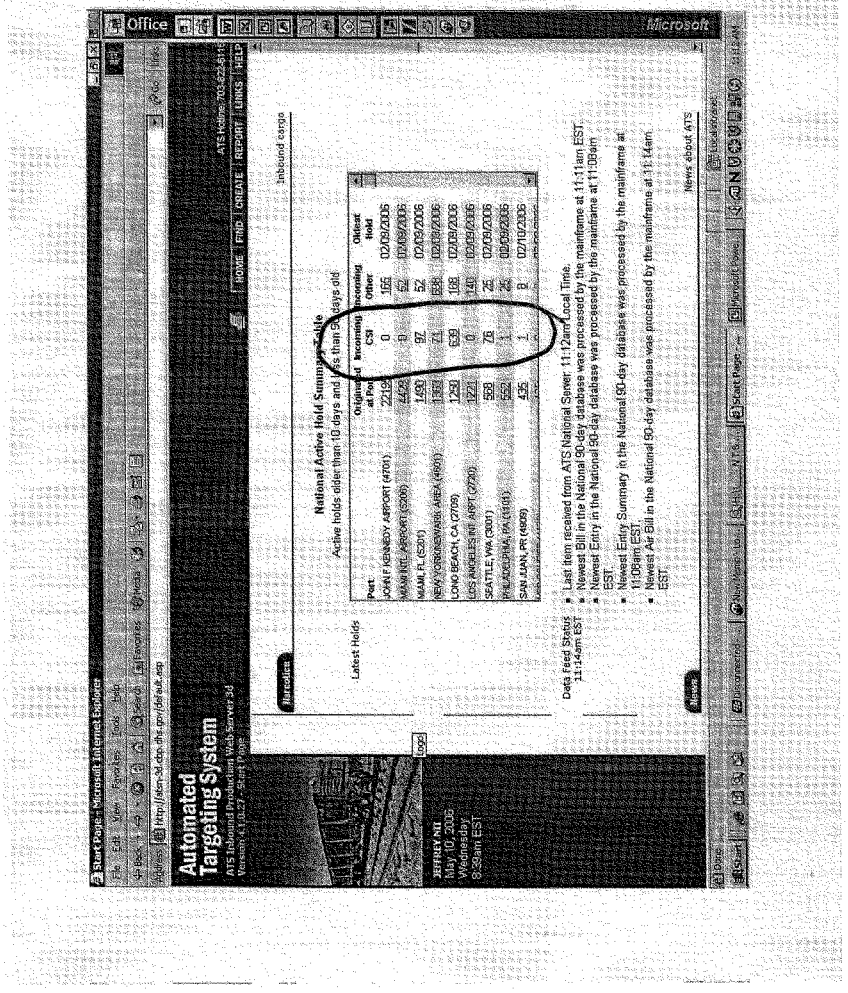
(3) CBP is working to develop and implement a testing and simulation environment. CBP has established the infrastructure for a simulation environment and is currently programming the system interfaces. This environment will facilitate research and development of new targeting methodologies, and improve testing and evaluation of current rule performance.

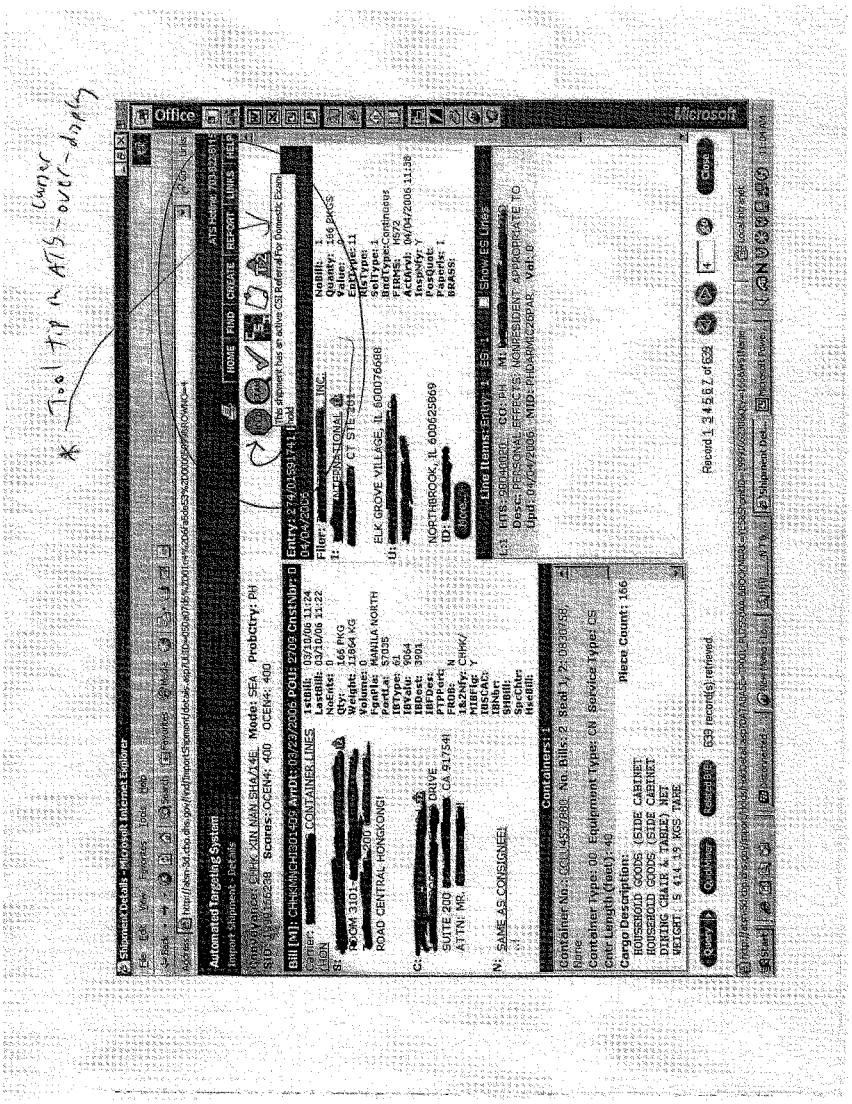
(4) CBP is addressing recommendations contained in a 2005 peer review of ATS.

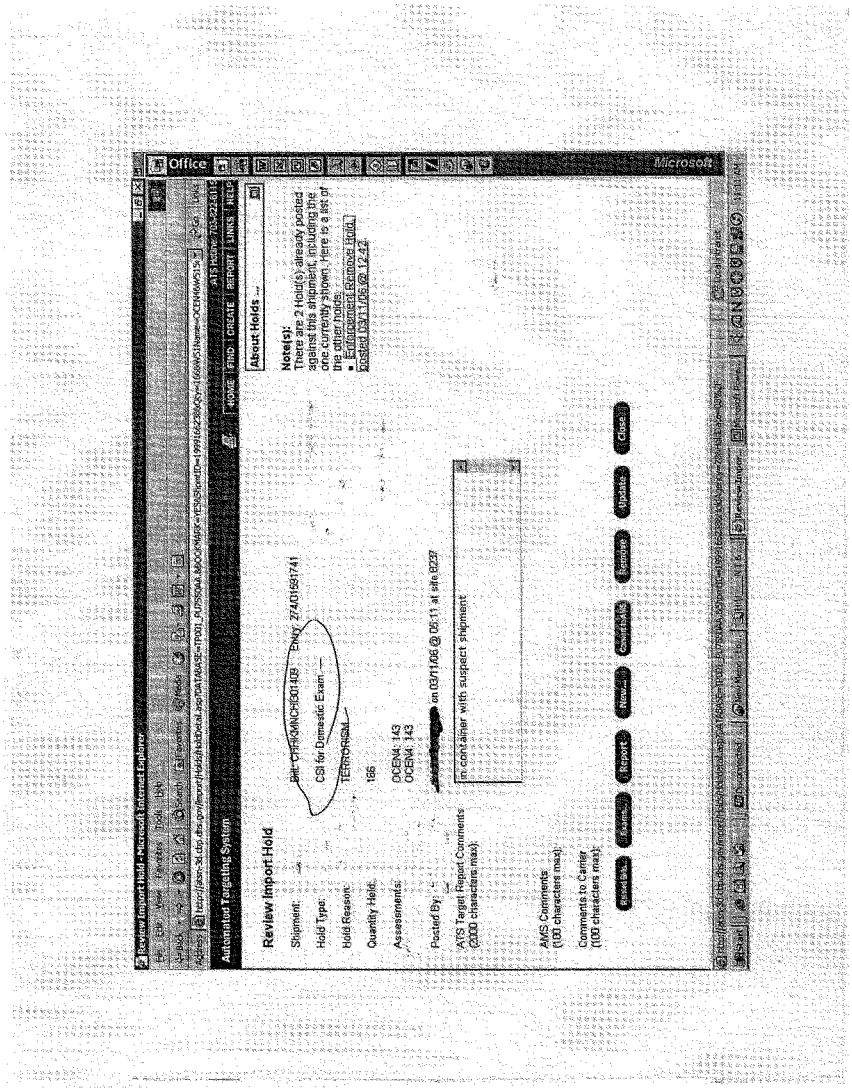
3. **At the hearing, I referenced a March 29th Detroit Free Press article (attached), *Security Lags When Traffic Jams,* which described a practice the article called "flushing," whereby CBP inspectors, at the instigation of their supervisors, allow trucks and cars to move immediately over the Ambassador Bridge, without being inspected, in order to move the bridge traffic quickly. Please comment on this article and whether or not "flushing" occurs at the Ambassador Bridge or other major border crossings in the country.**

Response: CBP does not currently have, nor has CBP had in the past, a policy or practice known as "traffic flushing." It is the priority mission of CBP to prevent terrorists and terrorist weapons from entering the United States, while also facilitating the flow of legitimate trade and travel. As part of their duties, CBP officers inspect all persons applying for entry to the U.S. to determine identity, citizenship, and right to enter or pass through the United States. CBP believes the statements in the article in the "Detroit Free Press" about CBP employees engaging in "traffic flushing" are inaccurate.

#


Automated Targeting System
ATS Inbound Production Web Server 3d
Inbound cargo
National Active Hold Summary Table
Active holds older than 10 days and
Latest Holds
Port
Original at Port
CSI
Incoming Other
Oldest Hold
JOHN F KENNEDY AIRPORT (4701)
2219
0
166
02/03/2006
MIAMI INTL AIRPORT (5300)
4426
9
62
02/03/2006
MIAMI, FL (5301)
1493
97
52
02/03/2006
NEW YORK/NEWARK AREA (4601)
1383
71
334
02/03/2006
LONG BEACH, CA (2709)
1259
639
108
02/08/2006
LOS ANGELES INT AIRPT (2720)
1221
0
141
02/06/2006
SEATTLE, WA (3001)
558
76
25
02/09/2006
PHILADELPHIA, PA (4101)
553
1
25
02/09/2006
SAN JUAN, PR (4809)
435
1
8
02/10/2006
Data feed Status
Last item received from ATS National Server: 11:12am Local Time.
Newest Bill in the National 90-day database was processed by the mainframe at 11:11am EST
Newest Entry in the National 90-day database was processed by the mainframe at 11:08am EST
Newest Entry Summary in the National 90-day database was processed by the mainframe at 11:08am EST
Newest Air Bill in the National 90-day database was processed by the mainframe at 11:14am EST
11:14am EST
News about ATS
Microsoft


Shipment Details - Microsoft Internet Explorer
Automated Targeting System
Import Shipment Details
Office
Microsoft
Tool tip in ATS - over-display


Review Import Hold
Shipment:
Hold Type:
Hold Reason:
Quantity Held:
Assessments:
Posted By:
ATS Target Report Comments: (2000 characters max):
AMS Comments: (100 characters max):
Comments to Carrier (100 characters max):
About Holds ...
Note(s):
There are 2 Hold(s) already posted against this shipment, including the one currently shown. Here is a list of the other holds:
Endorsement Remove Hold
Posted 03/11/06 @ 12:42
CSI for Domestic Exam
TERRORISM
186
OKBN4 143
OKBM 143
on 03/11/06 @ 05:11 at site 6237
In container with suspect shipment
Microsoft

Review Import Hold - Microsoft Internet Explorer

Automated Targeting System

HOME | FIND | CREATE | REPORT | LINKS | HELP

ATS Home 703-922-6116

About Holds ...

Review Import Hold

Shipment: Bill: CHHK9MCH4301409 Entry: 274/0159174

Hold Type: Enforcement Remove Hold — Accepted by AMS on 03/27/06 16:45

Hold Sub-type: NII Exam Completed

Hold Reason: HEADQUARTERS DIRECTED ACTION

Quantity Held: 166

Assessments: OCEAN 143
AT-N 745

Posted By: [redacted] on 03/11/06 @ 12:42 at site 2709

Removed By: [redacted] on 03/27/06

Note(s):
There are 2 Hold(s) already posted against this shipment, including the one currently shown. Here is a list of the other holds:
- CSI for Domestic Exam, posted 03/11/06 @ 05:11

ATS Target Report Comments (2000 characters max):

NII, CSI DOMESTIC EXAM REQUEST; NTC LOG# 170571

CSI OFFICER COMMENTS: the actual importer and shipper are the same. Unable to identify in any system. No address listed except for freight agencies. High risk.

AMS Comments: (100 characters max):

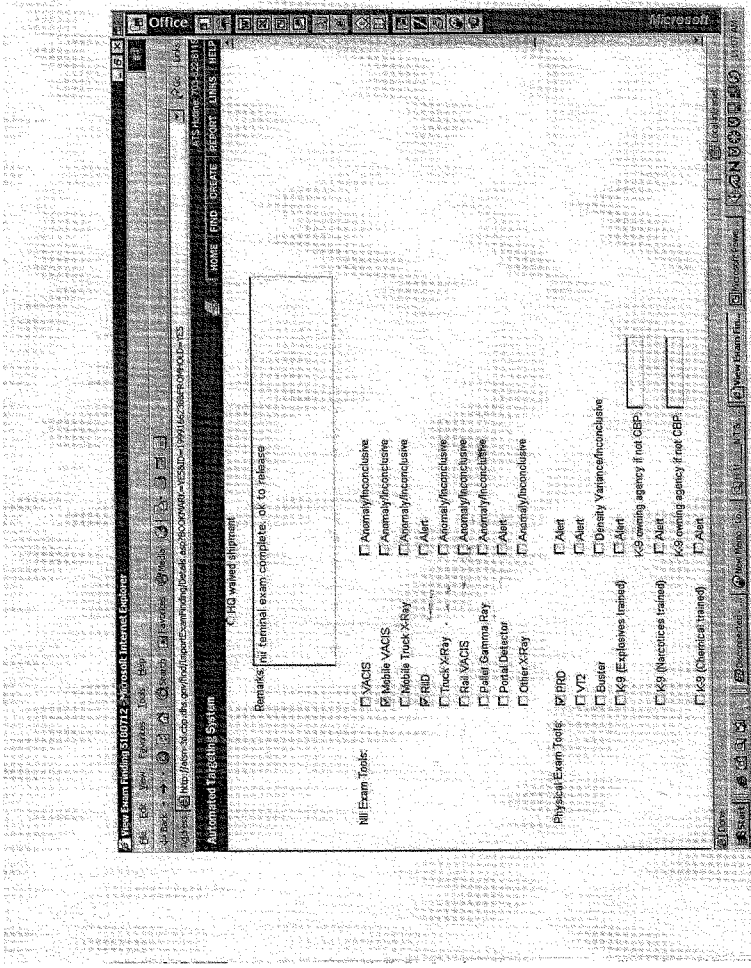
ATS HOLD: NII

Comments to Carrier (100 characters max):

AMS Removal Remarks: (100 characters max):

RELEASED VIA ATS

View Exam Finding 51860712
Automated Targeting System
HOME
FIND
CREATE
REPORT
LINKS
HELP
View Exam Finding 51860712
About Exam Findings
Record can be edited. Enter changes, then click Update to post.
NOTE: You must click UPDATE once all image uploading is complete, otherwise images will not commit.
Exam findings capture data from an inspection of cargo.
ATS will store your exam findings both in ATS and the ACS DEVAN file.
There are 2 Exams(s) already posted against this shipment, including the one currently shown. Here is a list of the other exams:
ID 5047922, 8237, 03/11/2006, Not Examined - Other
Shipment:
Bill: CHHKHKCHGH408 (1 Containers)
Entry: 234019917 41
Port of Unlading: 2709
Exam results apply to:
Bill of Lading (all entries)
Bill/Entry Pair
Specific Container:
Shipper:
Consignee:
MID:
Exam Status:
Exam record created by
on 03/27/2006
Exam Port: 2709
Examined — Specify outcome:
Exam Date: 03/27/2006 (e.g. MM/DD/YY)
Results: Positive Negative
New Seal Nbr1:
New Seal Nbr2:
If at CSI port, exam was observed by CBP personnel
Not Examined — Specify reason:
Data Analysis indicates Exam Not Warranted
Misdelivery
Reduced ATS Score
Shipment Diverted


View Exam Finding S160712 - Microsoft Internet Explorer
Automated Targeting System
HQ waived shipment
Remarks: Init terminal exam complete, ok to release
NII Exam Tools:
VACIS
Mobile VACIS
Mobile Truck X-Ray
RID
Truck X-Ray
Rail VACIS
Pallet Gamma Ray
Portal Detector
Other X-Ray
Anomaly/Inconclusive
Alert
Physical Exam Tools:
PRD
VI2
Buster
K-9 (Explosives trained)
K-9 (Narcotrices trained)
K-9 (Chemical trained)
K-9 owning agency if not CBP:
Density Variance/Inconclusive

Inspectors: Security lags when traffic jams

SPECIAL REPORT: Bridge operator pushes to keep border travel moving. Government officials deny cutting corners.

BY TAMARA AUDI
FREE PRESS STAFF WRITER

March 29, 2006

On a weekend night earlier this month, 12 big rigs from Detroit were lined up on the Canadian side of the Ambassador Bridge, waiting to be searched by inspectors who were on the lookout for a produce truck thought to be carrying drugs.

Traffic crosses the Ambassador Bridge earlier this month. Amid heightened terror concerns, about 9.4 million vehicles crossed the bridge in 2005, bridge officials said. (KATHLEEN GALLIGAN/Detroit Free Press)

But before the Canadians could scan the trucks, their supervisor received a call from the U.S. company that owns the bridge. The trucks were snarling traffic. And the bridge's owner wanted traffic cleared quickly, an inspector working that night said.

What happened next, according to customs inspectors and security experts, is what routinely happens on the U.S.-Canadian border when security clashes with commerce: Commerce wins.

"We stopped the inspection," a Canadian inspector said, and let the trucks pass.

Despite fears of terrorism and other security concerns at U.S. ports and border crossings since Sept. 11, 2001, U.S. and Canadian inspectors on the Ambassador Bridge and elsewhere say they are routinely told by supervisors to wave vehicles through checkpoints without scrutiny to satisfy commercial interests.

Though government officials in the United States and Canada deny safety is compromised, inspectors say security lapses are a particular problem at the Ambassador Bridge -- the busiest northern border crossing, and on of only two along the U.S.-Canadian border that are privately owned.

In one practice known as lane flushing, inspectors at the bridge -- owned by the Detroit International Bridge Co. - say supervisors force them to wave through long lines of cars and trucks to ease congestion, without asking even cursory questions of drivers or passengers.

"When the traffic backs up to a certain point, you know the call is going to come" from the bridge company, one bridge inspector told the Free Press. "Then management jumps like lapdogs."

Robert Perez, port director of Detroit for U.S. Customs and Border Protection, an agency of the Department of Homeland Security, denied lane flushing takes place. Perez said his office tries to cooperate with bridge and tunnel operators, and that inspectors might view that cooperation as caving in to commercial interests.

"The people in the community, both in Detroit and Windsor, should feel good about the fact that their border crossings are safer than ever before," Perez said.

The Free Press interviewed more than a dozen inspectors, former inspectors, Homeland Security officials, customs supervisors, politicians and border security experts -- including six inspectors assigned to the Detroit-Windsor border. All but one of the inspectors -- a Canadian union leader -- spoke on condition of anonymity, noting agency restrictions on media interviews and saying they feared job reprisals if named.

The allegations come as U.S. border security has faced its closest scrutiny since the 2001 terrorist attacks.

Congressional opposition recently scuttled a plan to have a Dubai-owned firm manage six U.S. ports. And Tuesday, as Congress debated tougher border security as part of an immigration package, a Senate subcommitte was investigating how undercover agents drove into the United States from Canada and Mexico with nuclear material.

Technology touted

U.S. and Canadian customs officials, and representatives from the bridge company -- owned by trucking magnat Manuel (Matty) Moroun -- insist security is never compromised for commerce and say, in fact, the reverse is true: Better technology, improved facilities and better cooperation between business and government make the border more secure and efficient.

Perez noted that the bridge and Detroit-Windsor Tunnel now feature high-tech surveillance -- invisible to travelers -- such as radiation detectors and electronic prescreening programs. And customs agents in Detroit seized more than 5,000 pounds of drugs last year, an eightfold increase over the previous year, he said.

Dan Stamper, president of the bridge company, said it has spent millions to expand facilities since 9/11 and would never ask inspectors to "give up any of their security initiatives to move traffic faster."

Bridge inspectors concede that, even under the best of circumstances, they could not fully inspect every vehicle entering the United States without crippling trade. Thus, they say, it is not unusual for drivers to pass inspection with only a few questions asked.

What they object to, they say, are orders from supervisors to wave through long lines of cars and trucks with no questioning at all. Sometimes, inspectors say, they have been told to stop inspecting a particular vehicle to open more booths when traffic backs up.

"They call and say, 'You're holding us up too much.' And they always win that argument," said Charles Showalter, national president of one of the two unions representing U.S. Customs and Border Protection officers

He said when inspectors or the union object, Homeland Security officials "call it 'acceptable risk.' It's 'Hurry up, hurry up, hurry up, hurry up.' Nobody wants to slow down commerce."

Bridge inspectors say this can happen once a week or more at the Ambassador Bridge -- one of two privately owned crossings on the U.S.-Canadian border. The other is a bridge in International Falls, Minn. However, they also say that inspectors are also pressured to speed traffic at government-owned crossings that are run by private companies.

The Detroit-Windsor Tunnel, for example, is run by a private company but owned by the City of Detroit on one side and Windsor on the other. Toll profits are shared with the cities.

Tolls collected at the Ambassador Bridge go to the bridge company, owned by Moroun of Grosse Pointe Shores.

Keeping the wait down

Since 9/11, traffic has declined about 30% at Detroit's border crossings.

To counter memories of long delays in the months after Sept. 11, the Detroit-Windsor Tunnel tries to keep waits under 20 minutes. Both the tunnel and bridge post wait times on their Web sites. During rush hour on an evening this week, bridge travel to and from Canada was under 15 minutes. The tunnel wait was under 6 minutes.

Neal Belitsky, executive vice president of the Detroit & Canada Tunnel Corp., which operates the tunnel, said he considers a 20-minute wait as "the outer limits for acceptability" for the roughly 29,000 vehicles that pass through daily.

"When we see traffic getting to that threshold, we will start calling customs and saying we need more lanes," he said. "That's a standard part of the business and we all do it."

He added there are times when customs denies his request and he backs off.

Danny Yen, spokesman for the Canadian Border Services Agency in Windsor, said, "We've had our challenges" with the bridge company, but "we never compromise security for trade. It's a balance."

Haste makes risk, some say

But inspectors say the rush to speed traffic has spawned practices -- such as lane flushing -- that put security at risk.

"Lane flushing happens all over the place, at every crossing," Showalter said. "The traffic backs up. The supervisor gets a call" from private border businesses. "They run an officer with a canine through the line of cars and the officers on the primary inspection lanes are told not to ask questions."

About 9.4 million vehicles crossed the Ambassador in 2005, according to bridge officials. Collectively, the bridge, tunnel and a commercial train tunnel account for nearly a quarter of all U.S. trade with Canada, the bulk of it by trucks crossing the bridge. When trade is delayed at the border, Michigan's automobile-reliant economy suffers most, a recent Ontario Chamber of Commerce study shows. Automakers use a "just-in-time" delivery system that depends on parts crossing promptly. A delay of even a few hours can cost millions.

A difficult balance

Perez, the Detroit port director, said changes intended to balance trade and security issues mean that some vehicles don't have to be checked as frequently. The government's so-called trusted traveler programs, for instance, allow prescreened businesses to cross faster and with fewer inspections, though critics say terrorists could exploit such efforts.

Colleen Kelley, president of the National Treasury Employees Union, a union representing 150,000 federal workers, including inspectors, said that pressure to speed trade means "something's got to give." What usually gives, she said, is thorough inspection work.

"The balance of trade and security became a battle that we really lost to trade years ago," said Joseph King, a professor and terrorism expert at John Jay College of Criminal Justice in New York who worked for U.S. Customs for 37 years. "Customs has become an honor system where the industry controls it, and periodically the government comes in and monitors."

And yet, ask Moroun -- whose company gets a reported $60 million annually in bridge revenue and spent $645,000 on lobbying and consulting over the past nine years -- about inspectors and he says, "They're very independent."

On the other side of the river, Marie-Claire Coupal, a Canadian customs inspector and local union leader, said she doesn't feel very independent lately. Of Moroun, she says, "He calls the shots around here."

The bridge company's Stamper responds that his firm has a duty to keep trade moving. And he notes that a recen study rated the Ambassador's travel times "clearly superior" to six other crossings.

Sept. 11, Stamper said, was a wake-up call for him, too. After the attacks, heightened security led to 14-hour bridge delays. Choking the economy was, after all, a major goal of the terrorists, he said.

So the main threat Stamper sees is not a dirty bomb, or suicide bombers. "Our biggest threat is our own government's reaction to the border."

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
SUBMITTED BY
SENATOR DANIEL K. AKAKA
to
THE HONORABLE MICHAEL P. JACKSON
Deputy Secretary
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 30, 2006

1. **In your testimony, you discussed the Department of Energy's Megaports initiative to improve our ability to detect nuclear and radiological threats overseas. Both the Domestic Nuclear Detection Office (DNDO) within the Department of Homeland Security and the National Nuclear Security Administration (NNSA) are charged with acquiring and deploying radiation detection equipment.**

   Can you tell how the DNDO works to complement, and not duplicate, Megaport and other Department of Energy initiatives and activities?

   Response: The question describes DNDO as "deploying" radiation systems. More accurately, DNDO supports the deployment of the systems by the operational DHS offices, such as CBP.

   The DNDO has the primary responsibility within DHS to integrate efforts across the Department to combat the threat of nuclear attack. This allocation of responsibilities is succinctly summarized as "centralized planning with decentralized execution." Through this management construct, the DNDO does not change any current roles, responsibilities, and functions of any Federal partner or infringe on the statutory responsibilities of partner agencies.

   Additionally, the DNDO is the lead Departmental representative for all interagency activities to coordinate the U.S. Government nuclear defense posture. As such, the DNDO works in close partnership with the Department of Energy (DOE) and its Megaports program to bolster, not duplicate, activities. For example, personnel from DOE serve as full-time detailees at DNDO, and are working on several activities, including the development of the domestic and global nuclear detection architecture and the creation of revolutionary radiation detection technologies. In addition, the DOE is a member of the Interagency Coordination Council (ICC) that serves as the DNDO's primary means to coordinate nuclear detection concepts and initiatives across the interagency.

At a strategic level, the DOE programs have been incorporated into the development of the global detection architecture. As the architecture evolves, the DNDO will put forward options and recommendations to the interagency community that improve our ability to detect radiological or nuclear threats. This includes working with Megaports at a programmatic level to close identified gaps in our layered defense.

Regarding technology development and acquisition, DOE NNSA and the DNDO are responsible for similar technologies that are utilized for complementary but different missions. NNSA responsibility includes research and development for international nonproliferation efforts, including intelligence gathering. The DNDO is responsible for protecting the U.S. through development of the global nuclear detection architecture to prevent radiological and nuclear materials from entering or transiting the country illicitly.

Some examples of collaboration include DHS and DOE joint participation in the interagency Domestic Nuclear Defense Research and Development (DNDR&D) Working Group, which is charged with creating an integral research and development roadmap addressing the entire domestic nuclear defense system. In addition, the planning process for the DNDO FY 2006 transformational research and development program included active participation from the DOE Nonproliferation and Verification Research and Development Program. Similarly, the DNDO supported the NNSA in reviewing foundational science proposals for advanced detectors and materials.

2. **I've been contacted by the National Treasury Employees Union (NTEU) because of their concern over a decrease in staffing levels within the Customs and Border Protection (CBP). More troubling, the President's Budget for fiscal year 2007 requests an increase of only $32 million and 21 full-time employees for all CBP operations at ports of entry. This stands in contrast with other human capital initiatives within the Department, including a $41.7 million or 133 percent increase for funding MaxHR, the new personnel system at DHS. I question the Department's commitment to address these critical staffing problems within CBP.**

   Can you tell me how CBP plans to address these staffing problems? Without a sufficient number of trained inspectors, how can we expect our borders to be protected?

   Response: CBP believes that it is adequately addressing staffing needs. For example, in addition to the increases you mention in Policy, Planning and Analysis for Border Security, Trade and Travel Facilitation at ports of entry, the FY 2007 President's budget proposal for CBP includes staffing and resource increases of 166 positions (83 FTE) and $18.8 million to enhance our ability to detect illicit radiological materials concealed within shipments, conveyances or containerized cargo entering the United States, and to support the physical expansion of the National Targeting Center (NTC) in support of

international passenger and cargo targeting operations. Details of these requested enhancements are as follows:

PPA: Inspection and Detection Technology (106 positions (53 FTE) and $12 million)
The additional staff will support the deployment of weapons of mass destruction (WMD) detection systems deployed through DNDO's WMD procurement program and ensure CBP will have dedicated personnel to resolve alarms from Radiation Portal Monitors (RPMs) and to conduct radiological examinations at our Nation's busiest seaports. These additional staff will ensure enough dedicated CBP personnel to conduct sufficient levels of WMD inspections at our Nation's seaports of entry and will be deployed to our 22 biggest seaports of entry. These top 22 seaports handle approximately 98% of the sea containers arriving in the United States.

PPA: National Targeting Center (60 positions (30 FTE) and $6.8 million)
The NTC directly supports all field enforcement activities related to the core anti-terror mission. Utilizing sophisticated targeting methodology, NTC staff analyze, screen, and target for intensive anti-terrorism inspection all passengers and cargo before arrival in the United States. Established in 2001 by CBP as the centralized location to manage national, tactical and strategic targeting, the NTC enables ports to focus more on continuous inspection operations while the NTC performs the necessary extended research and coordination. The additional positions requested in FY 2008 will support the expansion of the NTC to two sites in support of international passenger and cargo targeting operations in order to expand the NTC's overall anti-terrorism targeting, research and field support operations.

Currently, CBP determines the appropriate level of staff at our Ports of Entry (POE) by analyzing such criteria as: volume, processing times, facility constraints and expansions, number of terminals/lanes, threat and risk factors and overtime usage. CBP also solicits quarterly resource submissions from each Field Office to ensure that the proper staffing levels are allocated to where they are most needed. These quarterly submissions, combined with national and local initiatives and our current financial plan, are the current driving factors in the allocation of personnel.

In addition, CBP Office of Field Operations is taking proactive steps to ensure that staffing remains sufficient to meet mission critical needs, by developing an optimal staffing allocation model for CBP officers and Agriculture Specialists at POEs. This model will address staffing needs and adjust to changes in workload, processing time, complexity and threat levels. The primary output of the model will show a recommended level of staffing of CBP officers and Agriculture Specialists for each POE. The main methodology employed by the model is to calculate an expected level of workload based upon key workload elements and an associated required level of staffing to handle the workload at each location.

3. **Governor Thomas Kane testified that: "We are disappointed to hear, for example, that the FBI is not further along on preventing weapons of mass destruction."**

   Please describe how specifically the Department of Homeland Security works with the FBI to complement FBI efforts and initiatives designed to reduce nuclear and radiological threats to the nation?

   Response: The Domestic Nuclear Detection Office (DNDO), as the lead component within the Department of Homeland Security (DHS) for reducing nuclear and radiological threats to the Nation, works hand-in-hand with the FBI to complete its mission. The DNDO operating paradigm is one of "centralized planning with decentralized execution"—development of the global nuclear detection architecture occurs within the DNDO, but the FBI is specified as a primary law enforcement agency in the USG for response in many radiological and nuclear threat scenarios. On a more tactical level, the FBI provides full-time detailees to the DNDO, filling multiple roles in the DNDO including the Assistant Director for Operations Support and staff roles in the Office of Operations Support and the Office of Assessments. These daily interfaces ensure that the DNDO and FBI maintain continuous lines of communication and common awareness.

   The Homeland Security Operations Center (HSOC) is the primary national-level hub for domestic situational awareness, common operating picture, communications, information fusion, and operations coordination pertaining to the prevention of terrorist attacks and domestic incident management. The HSOC is a standing 24/7 multi-agency organization fusing law enforcement, national intelligence, emergency response, and private sector reporting.

   The below listed HSOC desks officers collect, share and coordinate nuclear and radiological threat information on a routine basis:
   FBI (Federal Bureau of Investigation)
   DNDO (Domestic Nuclear Detection Office)
   DOE (Depart of Energy)
   DOD (Dept of Defense)
   CBP (Customs and Border Protection)
   USCG (U. S. Coast Guard)

   The HSOC coordinates closely with the FBI Counter Terrorism Watch. There is an FBI desk in the HSOC Watch and the HSOC has a desk in the FBI Counter Terrorism Watch Center. Connectivity is crucial to the effectiveness of the liaison roles for all issues including the reduction of nuclear and radiological threats. The FBI HSOC desk officers have full access to their Automated Case System (ACS), email, as well as to the Guardian System. The latter system has been shared with other HSOC desk officers for anti-terrorism purposes to include attacks by nuclear and radiological threats. Whenever

the HSOC receives threats or suspicious activity reporting, especially Patriot Reports (reports from the public) which may be unique, the HSOC Senior Watch Officer ensures that the information is quickly disseminated to the FBI's Counter Terrorism Watch which sits at the National Counter Terrorism Center (NCTC). When there appears to be a nuclear or radiological threat, the HSOC coordinates information directly with the Weapons of Mass Destruction (WMD) Ops Unit of the WMD Section at FBI HQ. The WMD OPS Unit also maintains a 24/7 capability to coordinate a threat assessment procedure, using both in-house FBI and interagency subject matter experts, as appropriate, to ascertain the credibility of the threat. The nuclear or radiological threat information is also shared/coordinated with other agencies to include those listed above.

In addition, the DHS U.S. Immigration and Customs Enforcement (ICE) coordinates with the FBI in efforts and initiatives focused on the reduction of nuclear and radiological threats to the homeland. ICE and the FBI, along with other agencies such as Commerce, DoD, and State, complement each other's efforts in protecting the United States by preventing the illegal export of weapons of mass destruction technology from the U.S. Technologies illegally exported from the United States could be used to further foreign illicit state programs or terrorists' efforts to gain WMD capabilities. ICE has the broadest investigative authority to enforce United States exportation laws and export licensing requirements. These include authorities pertaining to dual-use technologies, U.S. Munitions List components, sanctions violations and related regulations. ICE and the FBI routinely coordinate on investigative matters to allow for the most comprehensive prosecution possible.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
SUBMITTED BY
SENATOR PETE DOMENICI
to
JAYSON P. AHERN
Assistant Commissioner
U.S. Customs and Border Protection

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

Q. The GAO has described their Red Team exercise by which they successfully smuggled radiological material utilizing falsified documentation. What measures can Customs and Border Protection take to enhance the effectiveness of portal detection equipment and to uncover falsified documentation?

Responses: As discussed in the hearing, the portal detection equipment functioned properly and the Officers followed established procedures. The outstanding issue, however, was that our Officers did not authenticate the legitimacy of the Nuclear Regulatory Commission (NRC) licensee/shipper information that the Investigators presented. U.S. Customs and Border Protection (CBP) has an established set of policy and procedures to address the issue raised by the Government Accountability Office. The following chronology describes events that led CBP – in conjunction with the NRC – to establish procedures for the verification of NRC licensee/shipper information.

On March 30, 2006, Customs and Border Protection and NRC managers met to discuss how to determine the legitimacy of NRC licensee/shipper information. Discussions centered on NRC/CBP roles and responsibilities, available licensee/shipper databases, and tentative solutions. The meeting concluded with scheduling a follow-up meeting.

On April 5, 2006, CBP issued an internal memorandum that directed all Field Officers to contact CBP's Laboratories and Scientific Services (LSS) Scientists whenever they required assistance in resolving the authenticity of NRC licensee/shipper information associated with the importation of industrial isotopes. As part of the process of resolving the legitimacy of NRC licensee/shipper information, LSS Scientists would act as the liaison with the NRC via a twenty-four hour hotline.

CBP and NRC managers reconvened on April 7, 2006, to discuss: the April 5 memorandum; the sharing of NRC licensee/shipper database information with CBP; CBP/NRC communication protocols; best/worse-case scenarios; and procedures for authenticating the

legitimacy of NRC licensees/shippers information. The meeting resulted in an agreement for the NRC to provide CBP LSS with NRC licensee/shipper databases, thereby enabling LSS to confirm discrepancies associated with licensee/shipper information. A process was also established in which LSS could verify discrepancies with the NRC via a twenty-four hour hotline.

On April 20, 2006, CBP LSS Scientists received the NRC databases and the NRC provided training on the use of the databases.

On April 27, 2006, CBP issued an internal memorandum reiterating the April 5, 2006 guidance, designating LSS as CBP's technical clearinghouse responsible for verifying NRC licensee/shipper information. The memo further delineated specific procedures to process and verify NRC licensee/shipper information and provided for instructions on processing travelers/passengers carrying industrial isotopes to be included.

Further meetings will be scheduled in the near future to follow-up on the adequacy of the established policy, agreements and procedures.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
SUBMITTED BY
SENATOR CARL LEVIN
for
VAYL OXFORD
Director, Domestic Nuclear Detection Office
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

Coordination between Megaports and Container Security Initiative

1. **Please explain what role the Department of Homeland Security has in coordinating the Department of Energy Megaports program and the Customs and Border Protection Container Security Initiative?**

   Response: The DNDO has the primary responsibility within DHS to integrate efforts across the Department to combat the threat of nuclear attack. Additionally, the DNDO is the lead Departmental representative for all interagency activities to coordinate the U.S. Government's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the Nation. As such, the DNDO works in close partnership with the DOE Megaports and the CBP Container Security Initiative (CSI) programs.

   At a strategic level, the efforts of Megaports and CSI are being included in the development of the global detection architecture. As the architecture evolves, the DNDO will work with Megaports and CSI to develop and implement options and recommendations to the interagency community that improve our ability to detect radiological or nuclear threats.

   For example, the DNDO works with DOE and CBP to encourage the use of advanced detection technologies at foreign ports. Some of these technologies are currently being created and tested through DNDO research, development, test, and evaluation programs. Furthermore, the DNDO has proposed the need for much more consistent and stringent information sharing requirements if U.S. funds are to continue to be used to deploy systems overseas. DNDO, through its Joint Analysis Center, will work with partners, like DOE and CBP, to secure agreements for more timely and uniform information sharing.

Global Architecture

2. **What is the global architecture that the Department of Homeland Security plans to establish for international border security and how will this be coordinated with the State Department, which has the lead responsibility in coordinating efforts to prevent nuclear smuggling overseas?**

Response: The DNDO has been tasked to develop the global nuclear detection architecture, but it alone will not be responsible for its implementation. That task will fall to other agencies, such as the Department of Energy and Customs and Border Protection, pursuant to current implementation agreements. Based on initial architecture analyses, DNDO has recommended that the following next steps should be considered: expand radiation screening opportunities within US international radiation detection security programs, upgrade deployed detectors and advise host countries on new response protocols and techniques, pursue greater integration of radiological and nuclear detection concepts into supply chain security initiatives, and secure agreements with host countries of all US deployed systems to provide greater access to detection information . Furthermore, the DNDO strongly recommends that the USG continue diplomatic efforts to develop country-specific strategies to reduce the risk of nuclear terrorism. These recommendations were briefed to, and agreed upon by, most interagency partners, including the State Department, as well as the White House (including the National Security Council).

Because the DNDO will not have implementation responsibilities for most of these initiatives, considerable effort has been made to involve interagency partners like the DOS in the development of proposed initiatives. The DNDO's responsibilities are succinctly summarized as "centralized planning with decentralized execution." Through this management construct, the DNDO does not change any current roles, responsibilities, and functions of any Federal partner or infringe on the statutory responsibilities of partner agencies. For example, the DNDO, in cooperation with the DOS, will develop methodologies and agreements with international allies in order to improve and expand the ability to conduct systems assessments against the outer layers of the global nuclear detection architecture.

Overall, the DOS has a key role in supporting the international activities of the global nuclear detection architecture. The DOS is a member of the Interagency Coordination Council (ICC) that serves as the DNDO's primary means to coordinate nuclear detection concepts and initiatives across the interagency.

3. **The GAO report, *Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries,* recommends that the National Security Advisory, acting through the National Security Council Staff issue a plan "guiding the implementation and coordination of threat reduction and nonproliferation programs addressing border security." How does the Global Architecture fit within this recommendation?**

   Response: The DNDO analysis of the baseline global nuclear detection architecture would complement GAO recommendations to create a national plan to address overseas border security. The global architecture identifies enhancements for the security posture of foreign borders and authorized ports of entry, and has produced an initial set of recommendations that could inform broader USG-related security programs at the source and foreign border security plans. For example, the DNDO strongly recommends integration of radiological and nuclear detection concepts into global supply chain security initiatives.

   The DNDO understands that coordination with relevant initiatives addressing vulnerabilities overseas (e.g. Second Line of Defense) is essential. Therefore, participating in joint-planning activities across the interagency is beneficial to and consistent with the process by which DNDO hopes to develop a global nuclear detection architecture.

Joint Center for Global Connectivity

4. **What is the Joint Center for Global Connectivity, what does it collect and how does it or will it improve the ability to prevent nuclear smuggling?**

   Response: The Joint Center for Global Connectivity has been recently renamed the Joint Analysis Center (JAC) to reflect not only the information sharing aspects of its mission, but the contributions it provides as an analytical component of the DNDO.

   The JAC will provide near real-time situational awareness of the global nuclear detection architecture, facilitate adjudication of nuclear detection events, and coordinate technical support to Federal, State, and local (F/S/L) authorities. In addition, the JAC fuses detection information and information generated by the intelligence and counterterrorism communities to provide a better-informed decision making environment, enabling more effective alarm resolution, trend analysis, and threat awareness. It is staffed by experts from the DNDO, DoD, DOE, FBI, USCG, CBP, and NRC.

   By monitoring the USG global nuclear detection system, the JAC provides 24/7 response for domestic radiological alarm resolution, including acting as a conduit from local authorities to national assets that can provide definitive spectrum analysis. Once fully operational, the JAC will coordinate domestic technical detection adjudication across the USG and facilitate communication between State and local agencies and Federal assets, enabling DNDO to

expedite domestic alarm resolution. However, the JAC will not duplicate the efforts of CBP's Laboratories and Scientific Services (LSS), but rather work directly with them for secondary alarm resolution.

A key component of the JAC is the Nuclear Assessment Program (NAP). The NAP is an ongoing weapons-lab based analysis program that assesses and reports on illicit trafficking of nuclear material, as well as nuclear threat communications. This capability provides the operator community, as well as decision makers, with more information about what they may or have encountered, enabling the F/S/L law enforcement, as well as other authorities, to better respond to nuclear related issues and incidents --- improving the Nation's ability to prevent nuclear smuggling. Using its technical, operational, and behavioral analysis capability of such events, it provides rapid, written assessments to support DHS, other members of law enforcement and the intelligence communities.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
SUBMITTED BY
SENATOR PETE DOMENICI
for
VAYL OXFORD
Director, Domestic Nuclear Detection Office
Department of Homeland Security

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

Q. Are the nuclear detection systems used at foreign ports the same systems used in the U.S.?

Response: US-funded overseas deployments under the Department of Energy Second Line of Defense / Megaports program, as well as other federal agencies security programs deploying radiation detection technology, utilize radiation portal monitors (RPMs). The currently fielded (US-funded) systems are technologically similar to those used at U.S. ports of entry, though equipment is provided by different vendors.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
Submitted By
SENATOR CARL LEVIN
to
DAVID G. HUIZENGA
Deputy Assistant Secretary
National Nuclear Security Administration

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

Coordination Between Megaports and Container Security Initiative

1. **Could you briefly describe the mission of the Megaports program, how it is coordinated with the Container Security Initiative, and the role of the Department of Homeland Security in coordinating the two programs?**

Response: The Megaports Initiative is an international nuclear security program under which DOE/NNSA cooperates with its foreign partners to enhance their capability to deter and detect illicit trafficking in special nuclear and other radioactive materials in the international maritime system. Under the Megaports program NNSA provides radiation detection systems, training in use of the systems, and technical and sustainability support to appropriate host nation law enforcement officials. Once installation, training, and system evaluation is complete, ownership of the equipment and responsibility for its operation transfers to the host government. The host government is obligated to provide all data associated with detections or seizures made as a result of the use of NNSA supplied equipment to the U.S. government.

As evidenced by the Memorandum of Understanding we signed with Department of Homeland Security's (DHS) Customs and Border Protection Bureau in April 2005, we are committed to maintaining a strong, effective partnership with the Container Security Initiative (CSI) program. We routinely and closely coordinate on the planning and implementation of the Megaports Initiative and the Container Security Initiative (CSI). The Megaports Initiative serves to enhance CSI targeting and scanning activities at foreign seaports by providing an additional scanning tool to detect nuclear and other radioactive materials in cargo containers prior to being loaded on vessels bound for the US. The broad extent of coordination between CSI and the Megaports Initiative is demonstrated by the 20 joint outreach missions and port assessments we have undertaken, the two joint agreements we have already signed with host governments, and our efforts to identify additional opportunities to jointly implement both programs. Finally, for the ports where CSI personnel are present, NNSA is developing procedures host country officials whereby CSI is directly notified of all alarms on containers bound for the U.S.

2. **Have you identified any additional steps that could be taken to improve coordination between the two programs, Megaports and the Container Security Initiative?**

Response: While we have a robust partnership in place, we are constantly looking for opportunities to leverage the strengths of each program. For example, we have recently signed joint agreements with Oman and Honduras (i.e., among CSI and the Megaports Initiative and foreign governments). We are pursuing additional joint agreements with host governments and hope to complete several such agreements over the next few months.

3. **It has been suggested that Megaports and Container Security Initiative be combined, could please address the pros and cons of this suggestion?**

Response: While some may argue that consolidating the two programs within one department will result in a more cohesive international port security policy, we believe this vision is already a reality through the extraordinary collaboration and coordination that NNSA and CBP have instituted between the Megaports program and CSI. The best way to accelerate overseas scanning of cargo containers is to continue to draw on the technical strengths in radiation detection at DOE/NNSA and the Customs experience at DHS and build on the already strong ties between these agencies.

There are a number of drawbacks to merging the programs. First, merging the two programs could result in lost opportunities to seize smuggled material or weapons because CSI is focused solely on screening U.S. bound containers. Although we are working towards the common goal of preventing WMD from entering our country, the Megaports program's mission is broader in that we are focused on detecting efforts to smuggle nuclear material, regardless of the destination.

Second, the Megaports Initiative is an integral component of our larger strategy to prevent the diversion of nuclear weapons and material. To reinforce our efforts to enhance the security of Russia's nuclear complex, the Second Line of Defense program deploys radiation detection systems at land borders, airports and seaports so as to provide numerous opportunities to deny terrorist organizations access to nuclear or other radiological material.

The National Security Presidential Directive (NSPD) that established the Domestic Nuclear Detection Office clearly acknowledged DOE/NNSA's role as the primary source of expertise in dealing with issues related to special nuclear and other radioactive materials. Leaving the Megaports program under NNSA will allow us to continue to leverage this expertise and build upon our solid record of successfully implementing nuclear security programs and managing related construction projects in foreign environments.

Finally, we are gaining significant momentum with 6 operational ports, implementation activities underway in 8 countries, and 6 more agreements are expected to be signed in 2006. NNSA has the contractual infrastructure in place and has purchased the radiation detection monitors to support these deployments.

Global Architecture

4. **The Department of Homeland Security plans to establish a global architecture for international border security. Will this global architecture impact the Department of Energy Megaports or other programs and how, if you know will the architecture be coordinated with the State Department, which has the lead responsibility in coordinating efforts to prevent nuclear smuggling overseas, and others in the Interagency working group?**

   Response: In coordination with the Departments of Energy, Defense and State, the DNDO is focused on developing the overarching multi-layered strategy to protect the U.S. from an act of nuclear terrorism, developing more advanced detection equipment, and examining methods to facilitate U.S. receipt of information on potential nuclear threats in near real-time. According to the terms of NSPD/HSPD that created this office, the Departments of Energy, State and Defense remain responsible for the policy and implementation of their respective international border security programs. The Domestic Nuclear Detection Office's (DNDO) responsibility to develop the global architecture for radiation detection does not obviate the need for the Department of State's coordination role. The Department of Energy continues to have the responsibility for the international deployment of radiation detection systems and will continue to consult with Department of State on its international cooperation programs. DOE is a participant in the Nuclear Trafficking Response Group (NTRG), which is chaired by Department of State and is responsible for facilitating the coordination of the U.S. Government response to all international-origin nuclear detection alarms.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
Submitted By
SENATOR PETE DOMENICI
to
DAVID G. HUIZENGA
Deputy Assistant Secretary
National Nuclear Security Administration

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

1. **Mr. Huizenga, in your testimony, you speak of a multi-layered approach to securing and detecting nuclear and radiological materials. Please describe the layers and how they are designed to work together to detect smuggled nuclear materials?**

   Response: By addressing the vulnerabilities at their source, NNSA's global nonproliferation programs form the "first line of defense" against the diversion of nuclear weapons and material through the installation of sustainable security systems at vulnerable nuclear facilities, the consolidation and return of nuclear material to secure locations, and the down-blending of excess nuclear material into forms that cannot be used for weapons. The detection systems deployed at high-risk land border crossings, airports and seaports under the Second Line of Defense (SLD) program provide a backstop to the nuclear site security systems, increasing the likelihood that any nuclear materials stolen from protected facilities is detected and interdicted. The SLD Megaports Initiative is specifically focused on prevent the global maritime shipping network from being used as a conduit for nuclear smuggling. As an integral element of the U.S. maritime security strategy, the Megaports program is closely coordinated with the efforts of the Department of Homeland Security's (DHS) Container Security Initiative (CSI) and complements the efforts of DHS' Customs-Trade Partnership Against Terrorism (C-TPAT), the Coast Guard's International Port Security Program (IPSP) and the Department of State's Proliferation Security Initiative (PSI).

2. **Some have argued that we should not place detection equipment in the hands of foreigners at international ports. Please describe the measures that are taken to build partnerships with foreign governments and port operators and to operate nuclear detection equipment.**

   Response: In support of the Megaports Initiative objective to detect, interdict, and deter illicit trafficking of special nuclear and other radioactive materials through the global maritime shipping network, NNSA enters into agreements with host countries to provide them equipment, comprehensive training and sustainability support. Megaports agreements dictate that host government officials are responsible for the operation and maintenance of

the equipment and adjudicating and responding to all alarms. Our foreign partners are further obliged to notify the U.S. Government of all detections and/or seizures of illicit nuclear and other radioactive materials. While our agreements are always with host countries, the cooperation of terminal operators in foreign ports is also an important factor in the successful implementation of the Megaports program. To that end, NNSA engages the terminal operators early on in the negotiations with our foreign partners to ensure their buy-in and to determine the optimal placement of the detection systems. Additionally, in many cases, terminal operators and/or port authority representatives, receive specialized training on the Megaports concept of operations in place at the port. It should be noted that many of the port terminal operators are leading the charge to promote maximum-security standards in their ports since their livelihood depends on safe and secure operations.

Finally, host government customs officials are always directly responsible for alarm response under the Megaports Initiative. To address any potential issues of corruption, NNSA has instituted multiple layers of oversight associated with operating equipment to prevent tampering with the detectors or ignoring alarms. Typically, alarms are simultaneously transmitted to at least two locations in the port to provide redundancy and to reduce the likelihood that a host government official would ignore or circumvent an alarm. If someone in the host country tampers with the detection equipment customs officials get a signal and take appropriate action. Additionally, the host country government routinely shares technical information with the U.S. on the performance of the systems so that we are able to assess whether or not the equipment is being operated properly.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
Submitted By
SENATOR DANIEL K. AKAKA
to
DAVID G. HUIZENGA
Deputy Assistant Secretary
National Nuclear Security Administration

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

Q. Since your office and the Domestic Nuclear Detection Office within the Department of Homeland Security are charged with acquiring and deploying radiation detection equipment, can you please tell me how you work together to complement, and not duplicate, each others efforts?

Response: As the primary agency responsible for international deployment of radiation detection equipment, NNSA works closely with DNDO to shape the global nuclear detection architecture. We routinely exchange programmatic and technical information to determine how the efforts of the Second Line of Defense program, which includes the Megaports Initiative, can enhance the external layer of the Global Architecture. Finally, we also provide input on our operational needs to inform DNDO efforts to develop more advanced detection equipment. Finally, we are working closely with DNDO procurement officials to potentially join DNDO procurement vehicles, and thereby leverage our combined purchasing power to reduce overall costs to the taxpayers and accelerate our deployments.

#

RESPONSES TO SUPPLEMENTAL QUESTION FOR THE RECORD
Submitted By
SENATOR DANIEL K. AKAKA
to
CMDR. STEPHEN E. FLYNN (USCG-Ret.)
Jeane J. Kirkpatrick Senior Fellow for National Security Studies
Council on Foreign Relations

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
HEARING ON
NEUTRALIZING THE NUCLEAR AND RADIOLOGICAL THREAT: SECURING THE GLOBAL SUPPLY CHAIN
March 28, 2006

1. **Given the flaws in detection technology, and the sheer number of containers entering our ports on a daily basis, you recently remarked that, n the absence of very detailed intelligence, inspectors will be able to perform on the most superficial of examination. In your opinion, what more could our intelligence community do to support the container inspection process?**

Response: Perhaps the most important task the intelligence community should perform is to analyze the core assumptions that inform the risk management system that the Customs and Border Protection Agency is relying on to target its inspections. To the best of my knowledge, CBP targeting system has never been subjected to a dedicated comprehensive external review by intelligence and counter-terrorism professionals.

CBP current targeting system is built on its pre-9/11 efforts for combating smuggling and ensuring compliance with U.S. laws and regulations. The cornerstone of CBP risk assessment framework is to reduce the percentage of containerized shipments that warrant physical screening or inspection by identifying nown shippers who have an established track record of being engaged in legitimate commercial activity and playing by the rules. These known shippers are deemed to pose a low risk. Since 9/11, CBP has built on that model by extracting a commitment from shippers to follow the supply chain security practices outlined in the Customs-Trade Partnership against Terrorism (C-TPAT). As long as there is not specific intelligence to tell inspectors otherwise, shipments from C-TPAT companies are viewed as presenting little risk. In other words, for CBP, past performance is a predictor of future results.

The intelligence community should be tasked with assessing whether a risk-matrix developed for combating crime is appropriate for assessing the risk associated with terrorists exploiting or targeting intermodal containers. My analysis leads me to conclude it is not.

When it comes to warding off criminals, private companies can indeed put in place meaningful security safeguards that can deter criminals from exploiting legitimate cargo

and conveyances for illicit purposes. This is because good internal controls raise the risk over time that criminals that try and penetrate the operations of a legitimate company will be caught and their illicit enterprise will be shut down. Organized crime groups want to maximize their profits by sustaining ongoing conspiracies. As such they tend to gravitate towards the places where the controls are weakest, and law enforcement reach is only episodic.

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

Second, terrorists are likely to find it particularly attractive to target a legitimate company with a well-known brand name precisely because they can count on these shipments entering the United States with a only a cursory look or no inspection at all. It is no secret which companies are viewed by U.S. customs inspectors as rusted shippers. Many companies who have enlisted in C-TPAT have advertised their participation in press releases or with postings on their website. In public speeches, senior U.S. customs officials have singled out several large companies by name as model participants in the program. So all a terrorist organization need do is to find a single weak link within a rusted shipper complex supply chain, such as a poorly paid truck driver taking a container from a remote factory to a loading port. They can then circumvent the mechanical door seal and gain access to the container in one of the half-dozen ways well-known to experienced smugglers. Since inspectors view past performance as the primary indicator of current and future compliance, as long as the paperwork is in order, the compromised cargo container almost certainly will be cleared to enter a U.S. port without anyone ever looking at it.

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

Beyond this external review, the intelligence community simply needs to dedicate more resources to establishing an overseas human intelligence presence in seaports and within the intermodal transportation system where the risk of penetrating that system by criminal and terrorist organizations is greatest. It also needs to bolster its in-house analytical capabilities to monitor trends within global transportation and logistics networks. There is an appalling lack of understanding within U.S. intelligence circles on how these networks work in practice. Given the growing nuclear proliferation risk, this lack of analytical capacity is both an important national security issue and a homeland security one.

# # #

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.

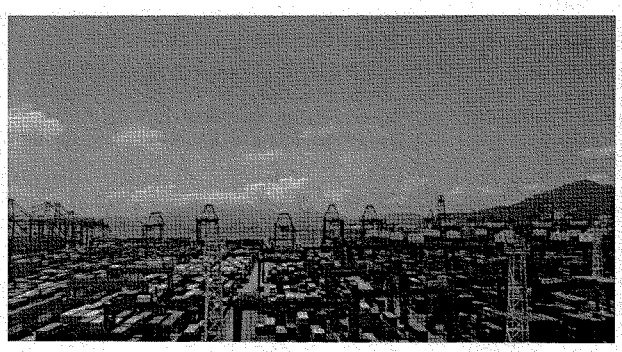


Figure 1. As the world's busiest port, Hong Kong illustrates the challenges of securing the global supply chain.

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.

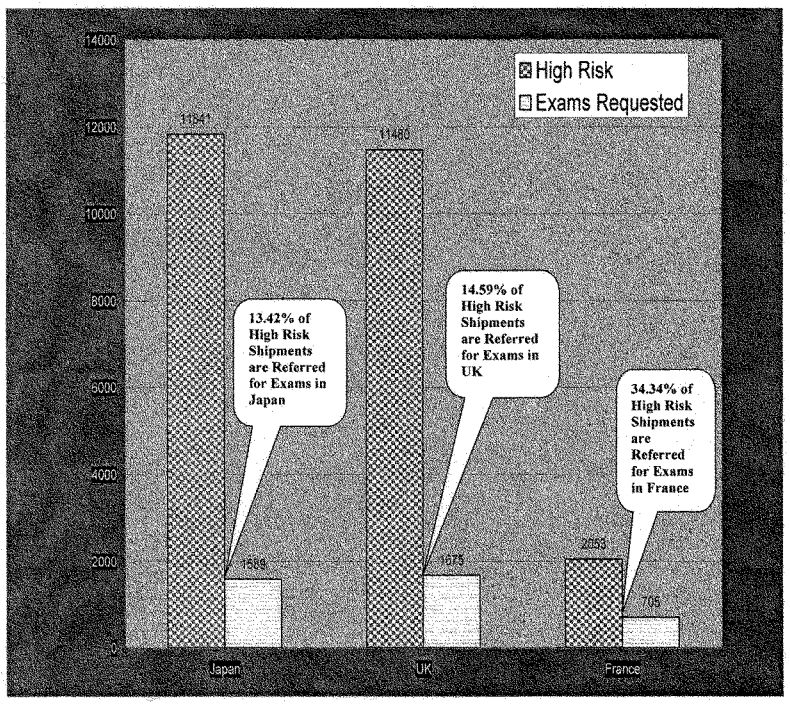
[35] CBP has never issued this order for security reasons; however, they have issued these orders for violations of the 24-hour rule.

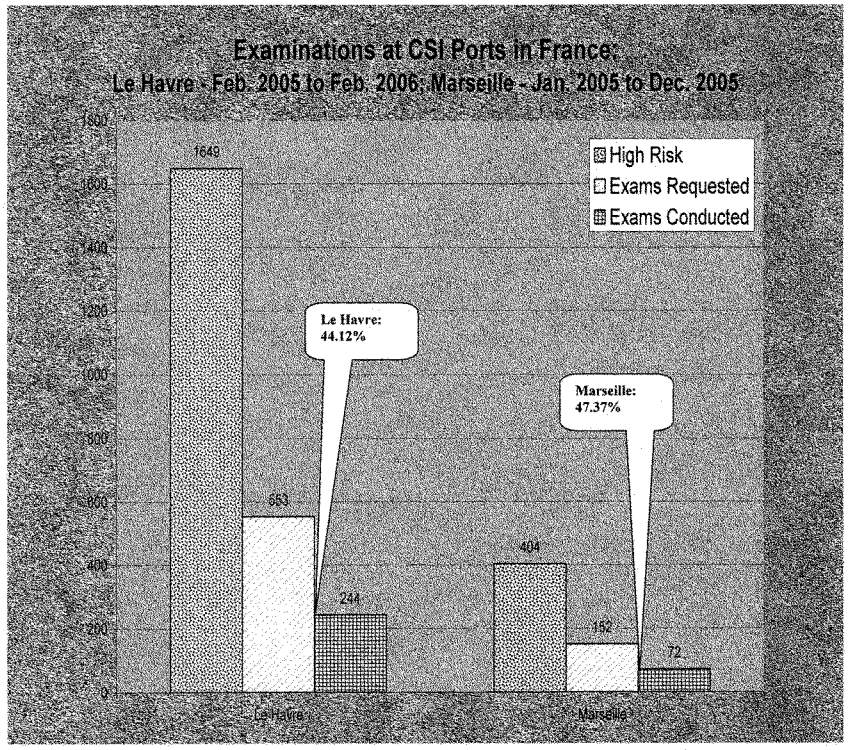
(e) Low Inspection Rates at CSI Ports

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.

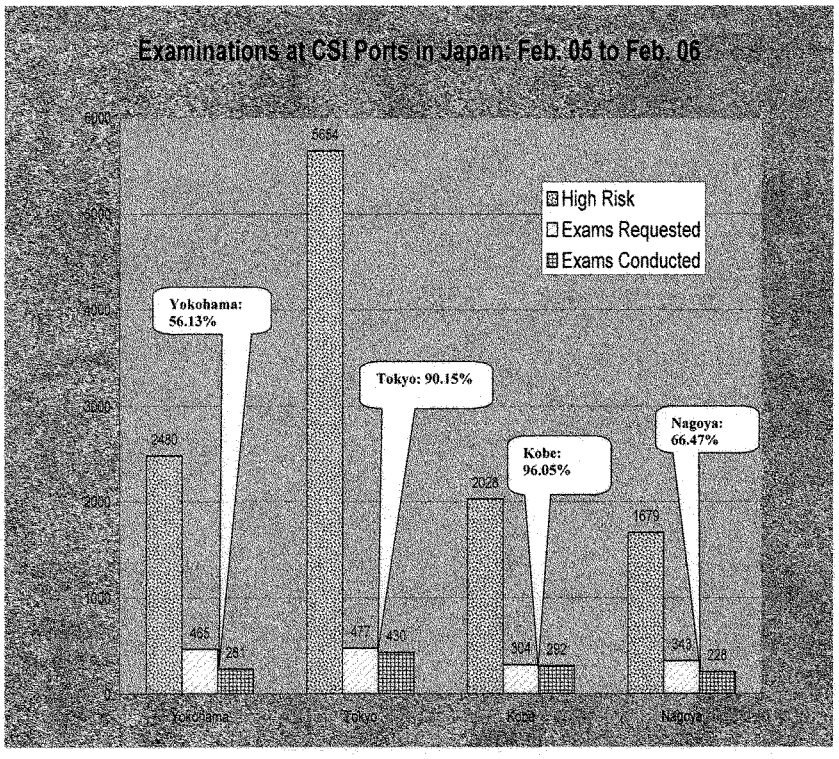




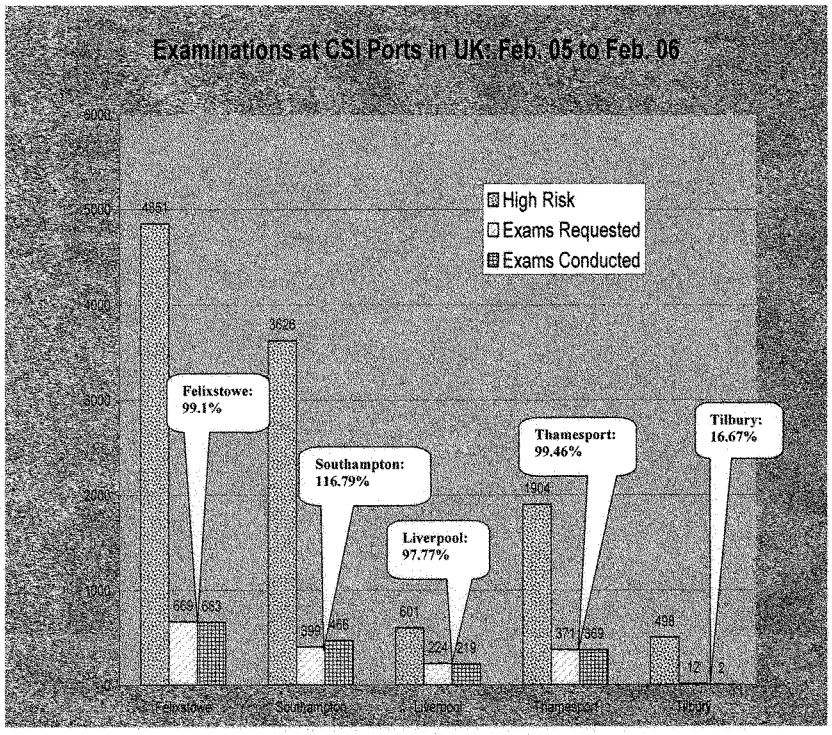
(ii) Inspection of CBP-Referred Containers Is Inconsistent

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.

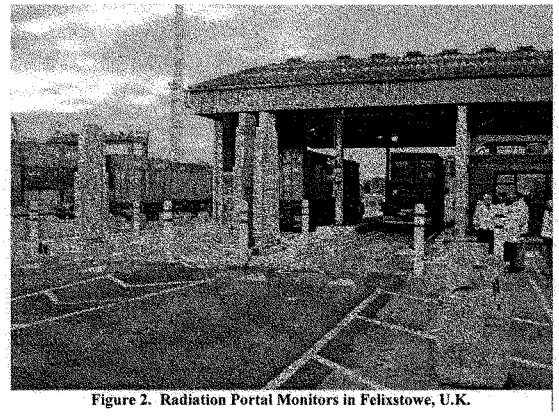


Figure 2. Radiation Portal Monitors in Felixstowe, U.K.

(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.

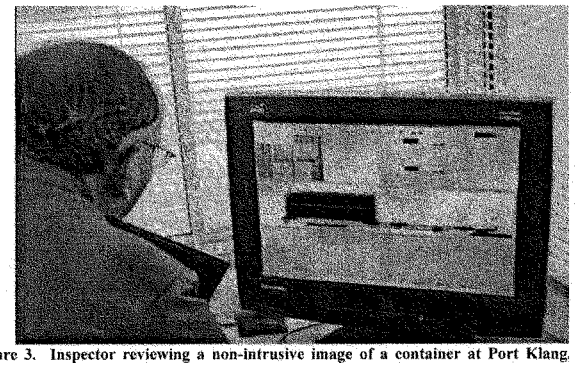


Figure 3. Inspector reviewing a non-intrusive image of a container at Port Klang, Malaysia

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.

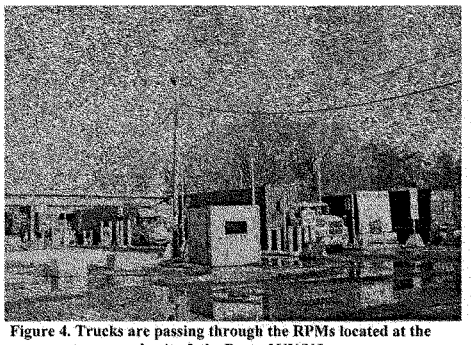


Figure 4. Trucks are passing through the RPMs located at the entrance and exit of the Port of NY/NJ.

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

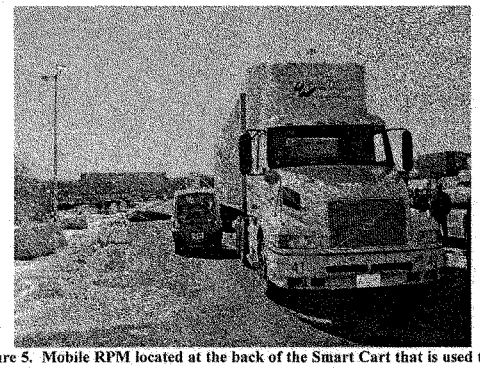


Figure 5. Mobile RPM located at the back of the Smart Cart that is used to determine the source of the radiation. After a truck alarms the RPM located at the entrance/exit to the Port, the truck is sent to the secondary inspection area.

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.

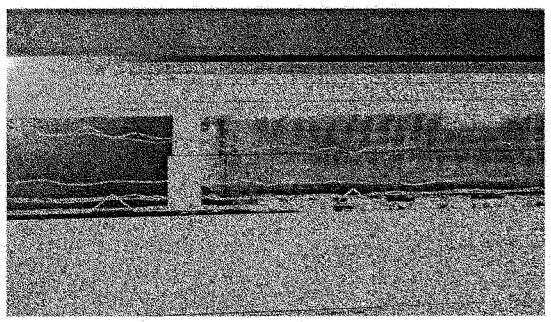


Figure 6. This ICIS image demonstrates the ability to view the RPM scan and x-ray simultaneously.

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.

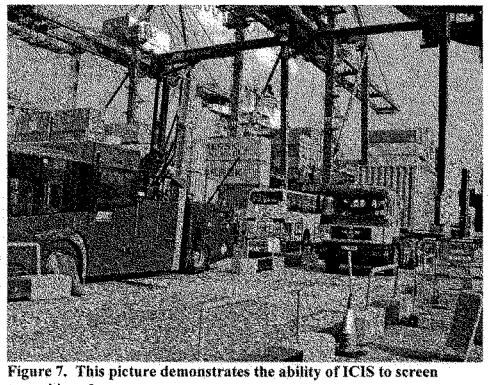


Figure 7. This picture demonstrates the ability of ICIS to screen transshipped cargo.

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.

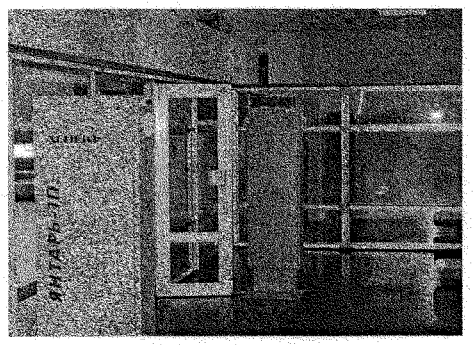


Figure 8. RPMs in Russia to screen air passengers and baggage.

(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