United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform

For Release on Delivery
Expected at 11:00 a.m. EST
in New York, New York,
Monday, November 18, 2002

# CONTAINER SECURITY

# Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges

Statement of JayEtta Z. Hecker
Director, Physical Infrastructure Issues

November 2002

# CONTAINER SECURITY

# Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges

GAO Highlights

Highlights of GAO-03-297T, a testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform

## Why GAO Did This Study

After the attacks of September 11th, 2001, concerns intensified over the vulnerability of U.S. ports to acts of terrorism. One particular concern involves the possibility that terrorists would attempt to smuggle illegal fissile material or a tactical nuclear weapon into the country through a cargo container shipped from overseas. This testimony discusses the programs already in place to counter such attempts, new initiatives now under way to enhance the nation's security against such attempts, and the key challenges faced in implementing these various efforts.

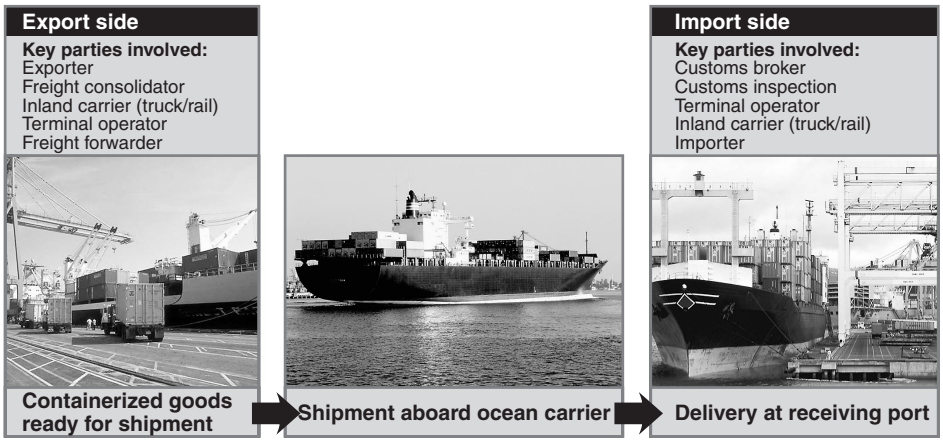
## What GAO Found

U.S. ports have programs in place to detect illegal fissile material or nuclear weapons, but these programs are limited in several respects. They focus on screening a small portion of total cargo as it enters the country, and they are carried out without the use of adequate detection aids, such as equipment that can scan entire containers for radiation. Efforts to target cargo for screening are hampered by the quality of information regarding which cargo poses the greatest risk.

New initiatives are under way to supplement these programs. The predominant focus of these initiatives has been to establish additional lines of security in the supply chain of international commerce. In essence, this means moving part of the security effort overseas, where goods are prepared for shipment into this country. These initiatives include such efforts as establishing international standards for ports, carriers, and maritime workers; stationing Customs personnel overseas; reducing security vulnerabilities all the way back to points of manufacture; and using new technology to monitor the contents and movement of containers from their point of origin.

The nation faces three key challenges to implementing efforts to improve the security of ports and containers: creating and enforcing a set of security standards, ensuring the cooperation of diverse groups with competing interests when it comes to the specifics of how things are to be done, and paying the increased security bill. Such challenges exist both for strengthening domestic efforts and for developing new initiatives that expand security on an international basis. GAO is currently reviewing several aspects of port and container security, and will report as those efforts are completed.

**Overview of Supply Chain for Cargo Containers**




Source: GAO, (c) Nova Development Corporation and Corbis Images (DigitalStock).

www.gao.gov/cgi-bin/getrpt?GAO-03-297T.

To view the full report, including the scope and methodology, click on the link above. For more information, contact JayEtta Hecker at (202) 512-2834 or heckerj@gao.gov.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here in New York City to discuss our work on efforts to address security risks related to U.S. ports. These risks are clearly serious ones that pose national security concerns. We have issued several reports and testimony statements related to nuclear smuggling and port security in general.

My testimony focuses on (1) the programs in place to prevent illegal fissile material or a tactical nuclear weapon from being smuggled into the United States through our ports; (2) new efforts under way to counter such smuggling, both domestically and abroad; and (3) the key challenges faced in implementing these various efforts. We have excluded information on these topics that has been deemed law-enforcement sensitive by the U.S. Customs Service (Customs), which precludes us from discussing it in an open hearing such as this. My remarks are based on completed GAO work on Customs efforts to detect hazardous materials at U.S. ports and federal efforts to secure U.S. seaports, as well as challenges involved in implementing these initiatives.[1] We are also presenting information based on ongoing work regarding new initiatives that address overseas supply chain security. See the appendix for a more detailed explanation of our scope and methodology.

In summary:

- The programs already in place at U.S. ports for detecting illegal fissile material or nuclear weapons are limited in a number of respects. They focus on screening a small portion of total cargo as it enters U.S. ports, and they are carried out without the use of adequate detection aids, such as radiation-detection equipment that can scan the entire contents of cargo containers. Instead, Customs personnel rely on small, handheld radiation pagers that have a limited range and capability. Other screening programs designed more broadly to identify any illegal or hazardous cargoes could potentially help identify such nuclear material as well, but these programs

[1]Previous GAO reports and testimony statements on these issues include *Nuclear Proliferation: U.S. Efforts to Combat Nuclear Smuggling Need Strengthened Coordination and Planning*, GAO-02-426 (Washington, D.C.: May 16, 2002); *Nuclear Proliferation: U.S. Efforts to Combat Nuclear Smuggling*, GAO-02-989T (Washington, D.C.: July 30, 2002); *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, GAO-02-993T (Tampa, FL: August 5, 2002); and *Customs Service: Acquisition and Deployment of Radiation Detection Equipment*, GAO-03-235T (Washington, D.C.: October 17, 2002).

rely heavily on the availability of quality information for targeting those cargoes posing the greatest risk. The Customs Service acknowledges that the accuracy of such information still needs improvement.

- The predominant focus of most new initiatives has been to establish additional lines of security in the supply chain of international commerce. In essence, this means moving part of the effort overseas, where goods are prepared for shipment into this country. These initiatives include such efforts as establishing international standards for ports, carriers, and maritime workers; stationing Customs personnel overseas to identify high-risk containers before inspection in foreign ports; reducing security vulnerabilities along the overseas portion of the supply chain; and using new technology to monitor the contents and movement of containers from their points of origin. Because the United States functions in a global economy where international organizations are addressing similar issues, current U.S.-led efforts are evolving within that context.

- The United States faces considerable challenges to successfully implement these existing and new efforts, both at home and abroad. Our reviews of port security programs have shown that even on the domestic front, the federal government faces challenges in creating and enforcing a set of security standards, ensuring the cooperation of diverse groups with competing interests when it comes to the specifics of how things are to be done, and paying the increased security bill. Our preliminary work indicates that these same challenges are likely to exist in efforts to extend strong measures of security elsewhere. To make its programs work, the United States is participating in and seeking to achieve consensus through a variety of international organizations, across many countries.

## Background

Seaports are critical gateways for the movement of international commerce. More than 95 percent of our non–North American foreign trade arrives by ship. In 2001, approximately 5,400 ships carrying multinational crews and cargoes from around the globe made more than 60,000 U.S. port calls. More than 6 million containers (suitable for truck-trailers) enter the country annually. Particularly with "just-in-time" deliveries of goods, the expeditious flow of commerce through these ports is so essential that the Coast Guard Commandant stated after September 11th, "even slowing the

flow long enough to inspect either all or a statistically significant random selection of imports would be economically intolerable."[2]

As indispensable as the rapid flow of commerce is, the terrorist attacks of September 11th have served to heighten awareness about the supply system's vulnerability to terrorist actions. Drugs and illegal aliens are routinely smuggled into this country, not only in small boats but also hidden among otherwise legitimate cargoes on large commercial ships. These same pathways are available for exploitation by a terrorist organization or any nation or person wishing to attack us surreptitiously. The Brookings Institution reported in 2002 that a weapon of mass destruction shipped by container or mail could cause damage and disruption costing the economy as much as $1 trillion.[3] Port vulnerabilities stem from inadequate security measures as well as from the challenge of monitoring the vast and rapidly increasing volume of cargo, persons, and vessels passing through the ports. Against this backdrop, it is not surprising that various assessments of national security have concluded that the nation's ports are far more vulnerable to terrorist attacks than the nation's aviation system, where most of the nation's efforts and resources have been placed since September 11th.[4]

Guarding against the introduction of nuclear or other dangerous cargo into the United States involves having effective security measures at numerous points along the supply chain. Transporting a shipping container from its international point of origin to its final destination is a complex process that involves many different participants and many points of transfer. Many of these participants carry out their roles in the exporting country (see fig. 1). The actual materials in a container can potentially be affected not just by the manufacturer or supplier of the material being shipped, but also by carriers who are responsible for getting the material to a port and by personnel who load containers onto the ships. Others who interact with the cargo or have access to the records of the goods being shipped include exporters who make arrangements for shipping and loading, freight

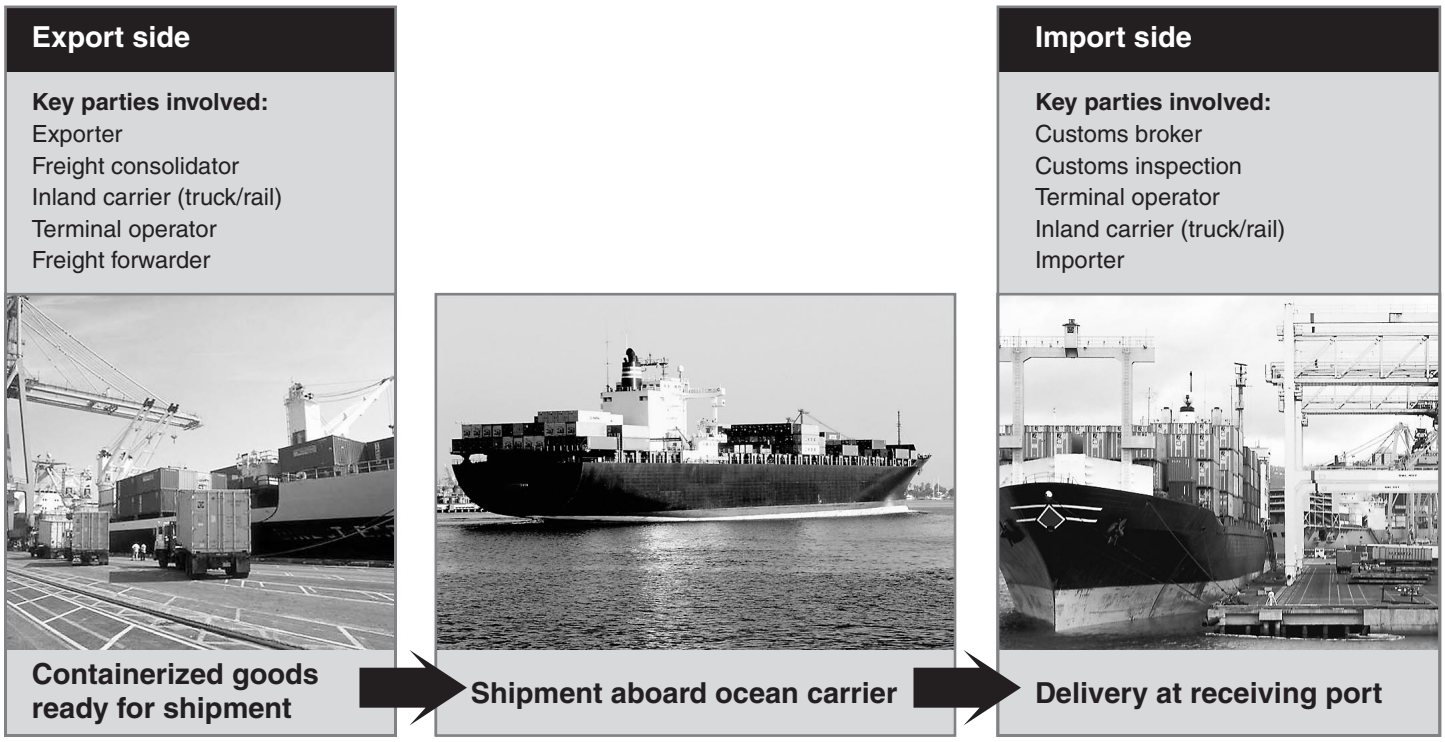
[2]Admiral James M. Loy and Captain Robert G. Ross, U.S. Coast Guard, *Global Trade: America's Achilles' Heel* (February 2002); and *Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response* (September 2001).

[3]Michael E. O'Hanlon et al., *Protecting the American Homeland: A Preliminary Analysis*, Washington, D.C.: Brookings Institution Press, 2002.

[4]Independent Task Force Sponsored by the Council on Foreign Relations, *America Still Unprepared—America Still in Danger*, October 2002.

consolidators who package disparate shipments into containers, and forwarders who manage and process the information about what is being loaded onto the ship. Review by the Customs Service, which traditionally comes once the ship arrives at its destination, is likewise just one step in the transportation chain on the domestic side.

**Figure 1: Overview of Supply Chain for Cargo Containers**




Source: GAO, © Nova Development Corporation and Corbis Images (DigitalStock).

Detecting smuggled fissile material that could be used to make a nuclear weapon is a difficult task not just because it is a potential needle in this vast haystack of international trade. It is also difficult because one of the materials that is of greatest concern—highly enriched uranium—has a relatively low level of radioactivity and is therefore very difficult to find with radiation-detection equipment. By contrast, radioactive materials that could be used in conjunction with conventional explosives to create a so-called dirty bomb are somewhat easier to detect, because they have much higher levels of radioactivity. Because of the complexity of detecting nuclear material, the Customs officers or border guards who are

responsible for operating the equipment must also be trained in using handheld radiation detectors to pinpoint the source of an alarm, identifying false alarms, and responding to cases of illicit nuclear smuggling.

## Existing Programs for Countering Nuclear Smuggling at Domestic and International Ports Are Limited

Existing programs for detecting the smuggling of nuclear materials are spearheaded by the Customs Service and are directed mainly at the import side of the transportation chain. Some of these efforts focus specifically on detecting nuclear materials, while others are directed at the wider range of hazardous and illegal shipments. In addition, several other federal agencies have efforts under way that are directed at the export side of the transportation chain—that is, at detecting and stopping shipments of nuclear materials before they leave the country of origin. We and others have pointed out that these programs lack many components, such as the best detection technology, for providing a more effective deterrent.

### Efforts Aimed Specifically at Detecting Nuclear Cargo Entering U.S. Ports

The Customs Service currently has some equipment in place for detecting radioactive or nuclear materials in the nation's ports and has begun training its agents to recognize and respond to radioactive materials. However, this equipment has limited effectiveness, and the agency's training programs, among other things, have not been integrated into a comprehensive plan.[5]

Customs' current screening program is based on several types of radiation-screening technology, only some of which are up and running:

- **Radiation-detection pagers**. Customs acquired radiation-detection pagers, which are worn on a belt, have limited range, and were not designed to detect weapons-usable radioactive material. Customs has deployed about 4,200 pagers among its 7,500 inspectors and expects every inspector to have a pager by September 2003. According to experts with whom we have spoken, these pagers are more effectively used in conjunction with other detection equipment rather than as a primary means of detection.

[5] *Customs Service: Acquisition and Deployment of Radiation Detection Equipment*, GAO-03-235T (Washington, D.C.: Oct. 17, 2002). We are continuing to conduct work on this issue.

- **X-ray–compatible detectors**. These radiation detectors are installed on X-ray machines that screen small packages. Customs has installed about 200 such detectors nationwide at border crossings and ports of entry. These detectors are not large enough to screen entire containers or other large cargo, however.

- **Portal monitors**. These detectors, which are not yet in place in ports or other points of entry, are larger than those on X-ray machines and are capable of screening the entire contents of containers, cars, or trucks. Customs is now completing a pilot test of such a monitor at one border crossing, and Customs officials told us that they plan to purchase up to 400 portal monitors by the end of fiscal year 2003.

According to Customs, about 5,000 of its approximately 7,500 inspectors have been trained to identify materials and components associated with the development and deployment of nuclear weapons. Customs also plans to give specialized training in the detection of nuclear material to as many as 140 of its inspectors, in cooperation with the Department of Energy's national laboratories. However, Customs has not yet developed an overall plan that coordinates equipment purchases and personnel training. Such a plan would also address such things as vulnerabilities and risks; identify the complement of radiation-detection equipment that should be used at each type of border entry point—air, rail, land, and sea—and determine whether equipment could be immediately deployed; identify longer-term radiation-detection needs; and develop measures to ensure that the equipment is adequately maintained.

## Efforts Focused More Broadly on Detecting All Hazardous Cargoes in U.S. Ports

Customs has methods and machines that, although directed more broadly at various types of hazardous or illegal cargoes, can be useful in finding radioactive and nuclear materials. These efforts are based largely on an approach of targeting a small percentage of containers for in-depth screening. With more than 6 million containers a year entering U.S. ports, examining them all has not been possible. Instead, Customs has acknowledged that its approach relies on reviewing shipping manifests, invoices and other commercial documents, and intelligence leads to target approximately 2 percent of the containers that enter the country nationwide for physical inspection, though the actual percentage varies from port to port. To better address terrorist threats, Customs is modifying its targeting approach, which was originally designed for counter-narcotics efforts. Customs officials told us that one of their greatest needs was for better information to more accurately target shipments. In a separate effort, GAO is conducting a review of Customs' processing of sea-borne

containerized, bulk, and break-bulk cargo bound for the United States,[6] focusing on targeting criteria, procedures, and the use of screening technology. On the basis of our preliminary work, GAO has identified a number of challenges related to the implementation and effectiveness of Customs' initiatives to ensure the security of cargo entering U.S. seaports. Customs has deemed the information we are collecting about that work as law-enforcement sensitive, which precludes our discussing it in an open hearing such as this.

To inspect the containers they target for closer scrutiny, Customs inspectors use gamma ray and X-ray machines that are capable of scanning the interior of a 40-foot container in less than a minute. The Port of Newark has four such machines, called VACIS machines.[7] Starting in the summer of 2002, Customs began deploying an additional 20 mobile gamma ray imaging devices at U.S. ports to help inspectors examine the contents of cargo containers and vehicles.[8] If necessary, containers can also be opened and unloaded for a lengthy, more thorough item-by-item inspection.

## Efforts in Nation's Ports Remain a Key Line of Defense

Aside from Customs' efforts, the Coast Guard and other agencies are undertaking a number of other fundamental actions domestically to improve our line of defense. For example:

- The Coast Guard has its own screening process for identifying and boarding vessels of special interest or concern. Shortly after the September 11th terrorist attacks, the Coast Guard modified its ship arrival notification requirement. The modification requires all vessels over 300 gross tons to contact the Coast Guard 96 hours—up from 24 hours—before they are scheduled to arrive at a U.S. port. Each vessel must provide information on its destination, its scheduled arrival, the cargo it is carrying, and a roster of its crew members. The information, which is

[6]Bulk and break-bulk cargoes include liquid bulk (such as petroleum), dry bulk (such as grain), and iron ore or steel.

[7]VACIS is a gamma ray imaging system that uses radiographic images to help inspectors examine the contents of trucks, containers, cargo, and passenger vehicles for hidden contraband. Gamma ray systems are regarded as state-of-the-art for such applications.

[8]Major ports are scheduled to receive additional VACIS systems, Mobile Truck Gamma Systems, Mobile Truck X-ray systems, High Energy Sea Container X-ray systems, and Pallet Inspections Systems. Additional deployments of equipment are planned over the next several years.

processed and reviewed by the Coast Guard's National Vessel Movement Center, is used in conjunction with data from various intelligence agencies to identify "high-interest" vessels. Decisions on appropriate actions to be taken with respect to such vessels, such as whether to board, escort, or deny entry to them, are made based on established criteria and procedures.

- Coast Guard officials are continuing to conduct vulnerability assessments of the nation's ports. These assessments help identify where local ports are most susceptible to security weaknesses and provide a blueprint of actions that need to be taken to make the ports more secure.

- Individual ports are taking a number of actions, often using newly provided federal funding to help pay for them. Three Department of Transportation (DOT) agencies—the Maritime Administration, the Coast Guard, and the Transportation Security Administration (TSA)—recently awarded grants to 51 U.S. ports for security enhancements and assessments. For example, in 2002, the Port Authority of New York and New Jersey received $3.5 million for such activities as developing devices for scanning containerized cargo for radioactivity, conducting preparedness training, and installing camera surveillance systems.[9]

  But actions such as these and the systems now in place at local ports to effectively identify, intercept, examine, and deal with ships and cargoes that arouse suspicion, or otherwise do not meet established standards, remain a work in progress. The recent incidents at the Port of New York and New Jersey involving the *Palermo Senator* and the *Mayview Maersk* illustrate that basic questions remain about how actions should be carried out at domestic ports. In both cases, the Coast Guard had concerns about the vessels but allowed them to enter the port. In the case of the *Palermo Senator*, the ship remained at the dock for 18 hours after testing showed high levels of radioactivity.[10] For the *Mayview Maersk*, the ship remained at the dock for 6 hours while the Coast Guard checked for explosives.[11]

[9]More recently, Congress passed legislation authorizing an additional $125 million for port security grants, including $20 million for port incident training and exercises. According to a Maritime Administration official, the grant application process has not begun, but he expects that grant awards will be made in the April 2003 time frame.

[10]The ship was subsequently towed to a security zone 6 miles offshore, where inspectors found that the radiation was natural radiation emanating from the ceramic cargo.

[11]The inspection showed that containers had previously held explosive cargo, but no explosives were found aboard the ship.

These incidents illustrate the need for clearer definitions of responsibility and procedure. Port Authority of New York and New Jersey officials, for example, cited a need for clearer guidance on the conditions under which ships can be denied entry into U.S. ports and the protocols for where and how to examine and unload ships suspected of carrying explosives or weapons of mass destruction.

## Efforts Aimed at Intercepting Shipments before They Leave the Export Country

Finally, turning to efforts outside U.S. borders, our ongoing work indicates that U.S. agencies have taken steps to address nuclear smuggling by attempting to ensure that nuclear materials do not leave some other countries, especially the former Soviet Union. Under its Second Line of Defense program, the U.S. Department of Energy (DOE) has installed 70 portal monitors at 8 border crossings in Russia since fiscal year 1997. These 8 crossings are the first of about 60 sites in Russia where DOE plans to install such portal monitors. According to DOE officials, the monitors provided to Russia have resulted in more than 275 cases involving radioactive material, including contaminated scrap metal, irradiated cargo, and other materials. The State Department and Department of Defense (DOD) have also provided detection equipment and other assistance primarily to former Soviet countries.

In our July 2002 report, we noted a lack of effective coordination among the overseas assistance programs.[12] That is, DOE, DOD, and the State Department have pursued separate approaches to installing radiation detection at border crossings, leaving some crossings more vulnerable than others to nuclear smuggling. Moreover, according to agency officials, U.S. assistance has sometimes lacked effective follow-up to ensure that the equipment delivered was properly maintained and used. Some equipment has sat idle for months or years for want of final agreements, reliable power supplies, or appropriate placement. For example, some equipment given to Estonia sat in an embassy garage for 7 months while an agreement governing its release was finalized; portal monitors sat in the U.S. embassy in Lithuania for 2 years because officials disagreed about whether a new $12,600 power supply was needed to run them; and one portal monitor delivered to Bulgaria was installed on an unused road. In many cases, countries that have received U.S. radiation-detection equipment were not systematically providing information to U.S. agencies

[12] *Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling*, GAO-02-989T (Washington, D.C.: July 30, 2002).

about the nuclear materials they detect, making it difficult to determine the equipment's impact and effectiveness. DOE and other agencies providing the equipment have identified these and other problems and are taking actions to address them.

## New Efforts Are Under Way to Address the Entire Supply Chain

In responding to the ongoing challenges of preventing radioactive and nuclear materials from entering the United States, the federal government has recognized that it must take a multi-pronged approach, including changes on the domestic as well as the international front. Concentrating on a small percentage of all containers, even with efforts to target high-risk cargoes, may not provide sufficient coverage. To widen coverage without bringing international commerce to a virtual halt, federal agencies are beginning to address those parts of the overseas supply chain that have received relatively limited attention, including country of origin. The main thrust of several new initiatives has been to create multiple lines of defense by pushing security beyond U.S. docks to include points of departure and, ultimately, places of manufacture. This is a fundamental change that involves viewing cargo security as an international effort rather than a national effort. Recognizing the important role that international organizations play in setting standards and procedures to facilitate international trade and enhance the security of the global supply chain, the United States is participating in these forums to help achieve these dual goals. To develop such international efforts, part of the federal government's effort must be on the diplomatic front as it seeks to forge security-related agreements in international forums, such as the International Maritime Organization (IMO). As the federal government is engaged in this new approach, it is also attempting to improve the lines of defense inside our nation's ports. Although various efforts to do so are under way, these efforts are in their preliminary stages. Currently, we are conducting a separate review for the Senate Committee on Finance and the House Committee on Ways and Means of Customs' Container Security Initiative (CSI) and Customs Trade Partnership Against Terrorism (C-TPAT) programs, focusing on their efforts to address concerns about the vulnerabilities of the international supply chain without impeding global commerce. We have obtained data from Customs' headquarters and have begun foreign fieldwork.

## New Initiatives Focus on Enhancing Security of Overseas Supply Chain

The fundamental shift in the approach to cargo security means that a program must be developed to put in place the additional checkpoints and procedures needed in the supply chain. The Customs Commissioner has emphasized the importance of such an effort in testing for the cargoes, stating, "If a cargo container has been used to smuggle a weapon of mass destruction set to go off upon arrival in the United States, it may be too late to save American lives and the infrastructure of a great seaport. Accordingly, we must change our focus and alter our practice to the new reality."

On this front, three primary initiatives are under way. Although all three initiatives focus on activities that affect the overseas supply chain, they differ somewhat in their focus and application.[13]

- The Container Security Initiative (CSI) focuses on placing U.S. Customs inspectors at the ports of embarkation to target containers for inspection.
- The Customs Trade Partnership Against Terrorism (C-TPAT) focuses on efforts by importers and others to enhance security procedures along their supply chains.
- The Operation Safe Commerce (OSC) focuses more heavily on using new technology, such as container seals, to help shippers ensure the integrity of the cargo included in containers being sent to the United States.

### CSI Places U.S. Customs Personnel in Foreign Ports

The CSI program that was announced in January 2002 is a new initiative intended to detect and deter terrorists from smuggling weapons of mass destruction via containers on ocean-going vessels before they reach the

[13]An additional effort, the outcome of which is classified as law-enforcement sensitive, is an interagency Container Working Group established by the Secretary of Transportation to address the security issues surrounding the movement of marine cargo containers through the international and intermodal transportation system. This effort is co-chaired by the Departments of Transportation and of the Treasury. According to DOT officials, the Container Working Group's activities are focused on information technology, security, business practices, and international affairs. On February 1, 2002, the group made recommendations to the Office of Homeland Security on ensuring the security of cargo container transportation. The recommendations addressed improving the coordination of government and business container security activities, enhancing cargo data collection, and improving the physical security of containers. The recommendations also support international container security efforts and the increased use of advanced technologies to improve the profiling of containers. In August 2002, a status report was forwarded to the Office of Homeland Security that detailed the progress on the twenty-four action items that were recommended in the original report.

United States. The United States is attempting to enter into bilateral agreements with foreign governments to place U.S. Customs personnel at key foreign seaports where, based on U.S. and foreign data, they will work with their foreign counterparts to target and inspect high-risk containers bound for the United States. By working at foreign ports with local customs, this program is designed to facilitate the early detection and examination of containers that are considered high-risk. Other key elements of CSI include developing criteria intended to enable Customs inspectors to better target high-risk containers suspected of transporting weapons of mass destruction, using technology to quickly screen high-risk containers at foreign ports, and developing and using smart and secure containers.

Customs is currently working to put such agreements in place. Customs has placed inspectors at 3 ports in Canada (Vancouver, Montreal, and Halifax) and is now focusing on efforts to cover the 20 ports with the highest volume of containers arriving into the United States. To date, eight governments, representing 13 of the top 20 ports, have entered into CSI agreements,[14] and Customs has placed inspectors in the Netherlands.[15] Agreements are currently under negotiation with six other governments, representing the remaining 7 ports. Customs also plans to expand the program to other ports deemed to be strategically important.

## C-TPAT Seeks to Improve Security Measures along the International Supply Chain

Another Customs initiative is the C-TPAT program, a partnership between the business community and Customs designed to enhance the security of international supply chains. Through this initiative, which began in April 2002, importing businesses, freight forwarders, carriers, and other logistics providers enter into agreements with Customs to voluntarily undertake measures that will reduce security vulnerabilities. Companies participating in the program must complete a self-assessment of their supply chain and submit to Customs a profile that describes their current security practices. Customs then reviews these profiles, certifies applicants, and provides them with feedback about security-related issues that need to be resolved.

[14]These ports are: Rotterdam in the Netherlands; Antwerp in Belgium; Le Havre in France; Bremerhaven and Hamburg in Germany; La Spezia and Genoa in Italy; Singapore; and Hong Kong. Japan has sealed the declaration of principles to participate in CSI by stationing, on a pilot basis, U.S. Customs officers at the ports of Tokyo, Nagoya, Kobe, and Yokohama. In addition, the Customs Service announced on October 25, 2002, that China is joining CSI, in principle.

[15]In December 2001, the Canadian Deputy Prime Minister and the U.S. Homeland Security Director signed the "Smart Border Declaration."

Once they are certified, C-TPAT members must still address Customs concerns on these issues. Customs plans to work jointly with companies to track their progress in making security improvements along their supply chains, but the emphasis is on self-policing rather than Customs verifications. Overall, Customs views the C-TPAT program as an incremental means to strengthen the international supply chain.

According to Customs, by participating in C-TPAT, certified importers and their supply chain partners could benefit from a reduced likelihood that Customs officials looking for weapons of mass destruction will delay the movement of their containers for inspection. Furthermore, in the event of an incident, C-TPAT members would likely be among the first allowed to resume their import operations.

As of early November 2002, approximately 1,100 companies had agreed to participate in C-TPAT, and Customs had certified 197 importers, 16 brokers, and 22 carriers. C-TPAT is currently open to all importers, brokers, freight forwarders, and non-vessel–owning common carriers, as well as most other types of carriers.[16] Customs, in consultation with private-sector partners, plans to expand the program to port authorities, terminal operators, warehouse operators, and foreign manufacturers.

## OSC Applies New Technology to Provide Greater Assurance That Cargoes Are Safe

OSC was initiated by the private sector as an attempt to make the supply chain more secure. OSC is administered by TSA within DOT and is funded by $28 million appropriated by the Congress in July 2002. Like the two Customs initiatives, OSC seeks to move the primary reliance away from control systems at U.S. ports of entry and toward improved controls at points of origin and along the way. OSC relies on using new technology such as electronic container seals to strengthen the security of cargo as it moves along the international supply chain. Efforts center on the following:

- ensuring that containers are loaded in a secure environment at the point of product origin, with 100 percent verification of their contents;

[16]C-TPAT is open to carriers involved in air, rail, and sea transportation as well as to U.S.-Canadian border highway carriers.

- using such technology as pressure, light, or temperature sensors to continually monitor containers throughout their overseas voyage to the point of distribution in the United States; and

- using cargo-tracking technology to keep accurate track of containers at all points in the supply chain, including distribution to their ultimate destinations.

The nation's three largest container port regions (Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma) are involved in the OSC pilot project, which will address the security vulnerabilities posed by containers entering these U.S. port regions. According to the port officials, they are working together with federal agencies to determine which procedures and technologies constitute the best practices in supply chain security. According to TSA, the OSC final grant award criteria will be contained in the Request for Applications, which is expected to be released in December 2002.[17]

## International Approach Requires Consensus-Building Efforts

According to the Associate Deputy Secretary of DOT, who serves as the principal policy adviser to the Secretary of Transportation as well as co-chair of the Operation Safe Commerce Executive Steering Committee, meaningful improvement in global transportation security will involve actions of many international organizations and governments. The Administration, including various federal agencies, is working with regional and global leaders and international organizations to further this critically important transportation security agenda. Key initiatives are being pursued in the International Maritime Organization, the World Customs Organization, the International Organization for Standardization, the International Labor Organization, and the United Nations Sub-Committee of Experts on the Transportation of Dangerous Goods.

### Seeking Consensus with Regional and Global Leaders

To encourage the broadest possible international consensus regarding the importance of enhancing transportation security on a global basis, the

[17]Separately from the OSC effort, the world's three largest seaport operators, representing 70 percent of the world's container traffic, are collaborating to demonstrate and deploy automated tracking detection and security technology for containers entering U.S. ports. Driven and initially funded by industry, this initiative, called Smart and Secure Tradelanes, is focused on container security and tracking and will be built on existing infrastructure and technologies that are proven, available for immediate deployment, and adaptable to emerging new technologies.

Administration has promoted a transport security agenda both at the most recent G8 Summit in Canada (June 2002)[18] and the recent meeting of Asia Pacific Economic Cooperation leaders in Los Cabos, Mexico (October 2002). DOT officials report that in both forums, participants endorsed the importance of adopting aggressive measures to combat the terrorist threat to transportation on a global basis—notably, through the work of international organizations—and to accelerate, where possible, the deadlines for implementation of important new requirements.

## Forming New Security Consensus through the International Maritime Organization

The International Maritime Organization is responsible for improving maritime safety, including combating acts of violence or crime at sea. The Coast Guard and DOT spearhead U.S. involvement in the IMO. Ninety-eight percent of the world's international shipping fleet operates under the agreements it promulgates. Following the September 11th attacks, IMO started determining new regulations needed to enhance ship and port security and to prevent shipping from becoming a target of international terrorism. Consideration of these new regulations is expected at a diplomatic conference scheduled for December of this year. According to Coast Guard officials, the new regulations will contain mandatory requirements for ships engaged in international voyages and for port facilities that serve such ships. The structure of the measures includes a family of plans. Port facilities and ships will assess their vulnerabilities and then develop security plans to address those vulnerabilities at specified threat levels. Port facilities and ships will also assign personnel as security officers to ensure development and implementation of these security plans.

According to a Coast Guard official participating in the IMO negotiations, IMO's work is central to much of the international strategy propounded by the administration and the Congress. For example, the Port and Maritime Security Act of 2001,[19] which is being finalized in conference committee action, calls for the Secretary of Transportation to assess the acceptability of foreign port security "based on the standards for port security and

[18]The G8 includes representatives from the governments of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, the United States, and the European Union.

[19]S. 1214, a bill introduced by Senator Ernest F. Hollings, was aimed at amending the Merchant Marine Act of 1936 to establish a program to ensure greater security for U.S. seaports; it passed in the Senate on December 20, 2001. The House version of S. 1214, the Maritime Antiterrorism Act of 2002, does not contain a similar requirement.

recommended practices of the IMO and other appropriate international organizations."

### Establishing Stronger Customs Procedures through the World Customs Organization

The World Customs Organization (WCO) is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of customs administrations. Among other things, WCO establishes and maintains international instruments to make customs procedures more uniform. In September 2002, WCO organized a task force that is expected to be the first step in developing new guidelines for supply chain security. The task force, which plans to complete its work by June 2003, will examine numerous security-related topics, including enhancement of import, export, and in-transit controls; improvement of technology; and development of better data and techniques for selecting which cargoes to inspect. The Customs Service is a participant on this task force.

### Developing New Security-Related Standards through the International Organization for Standardization

Although much of the framework for port security is established by these first two agencies, the International Organization for Standardization (ISO) is another important international body involved in improving international supply-chain security. ISO, a worldwide nongovernmental federation of national standards bodies from more than 140 countries, attempts to standardize various activities and products with a view toward facilitating the international exchange of goods and services. In this role, ISO would be responsible for developing standards for devices such as electronic container seals. ISO is currently participating in a pilot project dealing with these electronic seals.

### International Labor Organization Sets Requirements for Persons Working Aboard Ships

The International Labor Organization (ILO), a United Nations agency, is the agency that determines the requirements to be included in identification documents for seafarers. Still another aspect of the expanded security system involves checking on the background of crew members aboard ships transporting cargo destined for the United States. ILO and IMO have been working on the issue of seafarer documents since February 2002. Also, ILO may consider standards for port worker identification documentation.

### U.N. Sub-Committee of Experts on Transportation of Dangerous Materials

A senior DOT official reports that based on the G8 consensus of June 2002, the United Nations Sub-Committee of Experts on the Transport of Dangerous Goods (U.N. Sub-Committee) considered steps it could take to enhance security through international regulations on the transport of dangerous goods (hazardous materials). At its July 2002 meeting, the U.N. Sub-Committee agreed to consider specific measures for inclusion in the United Nations Recommendations on the Transport of Dangerous Goods

at its meeting in early December 2002. In preparation for the December meeting, the DOT Research and Special Programs Administration, which leads the U.S. delegation to the U.N. Sub-Committee, worked collaboratively with other governments to gain consensus on security requirements that could be accepted at the December meeting. These proposed amendments have now been formally proposed to the U.N. Sub-Committee through a United Kingdom submission.

The proposed amendments call for hazardous-materials employees to be trained in security at a level commensurate with their responsibilities, and it requires shippers and carriers of high-hazard materials to assess their security vulnerabilities and develop a security plan to address vulnerabilities identified. These requirements mirror those proposed by the Research and Special Programs Administration for inclusion in U.S. DOT Hazardous Materials Transportation Regulations, which are expected to be finalized later this year.

## Key Challenges Include Creating and Implementing Standards, Ensuring Cooperation of Diverse Groups, and Securing Resources

In our August 2002 testimony on security actions being taken to improve security within domestic ports, we found indications that there could be considerable challenges.[20] These include implementation of standards defining what safeguards should be in place and how they should operate, difficulties in establishing effective coordination among the many entities that have a stake in port security, and availability of sufficient funding to carry out the full range of actions that may be needed. The attempts to improve existing nuclear-detection programs and to implement the new initiatives now under way could face challenges domestically and internationally in these three areas as well. The United States is working through a variety of international organizations, each with a certain set of responsibilities, to establish consensus and to encourage compliance on security issues.

### Implementing Security Standards Could Prove Difficult

Adequate standards, consistently applied, are important because lax security at even a handful of ports could make them attractive targets for terrorists interested in smuggling dangerous cargo, damaging port infrastructure, or otherwise disrupting the flow of goods. On the domestic front, development of a set of national standards that would apply to all

[20] *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, GAO-02-993T (Washington, D.C.: Aug. 5, 2002)

ports and all public and private facilities is well under way. The Coast Guard, through a contractor, has been developing a set of standards since May 2002 as part of its efforts to conduct vulnerability assessments at 55 major U.S. ports. The standards will cover such things as preventing unauthorized persons from accessing sensitive areas, detecting and intercepting intrusions, checking backgrounds of those whose jobs require access to port facilities, and screening travelers and other visitors to port facilities. In the past, the level of security has largely been a local issue, and practices have varied greatly. The standards are to be performance-based, meaning that they describe the desired outcome and leave the ports considerable discretion in how to accomplish the task.

In our earlier work, we reported that effectively implementing such standards in U.S. ports, even with the authority of the federal government behind them, poses challenges. For example, at the Port of Tampa some major employers, such as ship repair companies, hire hundreds of workers for short-term projects as needs arise. Historically, according to port authority officials, these workers have included people with criminal records. However, new state requirements for background checks, as part of the credentialing process, could deny such persons access to restricted areas of the port.[21] From a security standpoint, excluding such persons may be advisable; but from an economic standpoint, a company may have difficulty filling jobs if it cannot include such people in the labor pool. Around the country, ports will face many such issues, ranging from these credentialing questions to deciding where employees and visitors may park their cars. To the degree that stakeholders disagree on specific methods, or believe that specific security actions are unnecessary or conflict with other goals and interests, achieving consensus about what to do will be difficult.

Developing and implementing standards across international lines is likely to present a formidable challenge as well, but doing so is essential to protecting the integrity of the international supply chain. Efforts to develop international standards are under way on several fronts, but much

[21]The House-passed version of S. 1214, the Maritime Transportation Antiterrorism Act, contains a provision that requires transportation security cards for entry to any secure area of a vessel or facility. The bill requires the Secretary of Transportation to issue a card to an individual who applies for one unless, after a background check, it is found that this individual poses a terrorism security risk. The Senate-passed version of this bill does not contain a similar provision, and it is unclear how the conference committee will decide this issue.

still remains to do. For example, security procedures for loading and sealing a container at the manufacturer's or consolidator's warehouse, or for transferring cargo from one mode of conveyance to another, are still under development. Likewise, international standards covering documentation on the contents of cargo containers and the credentialing of cargo handlers and port workers are still being discussed. Because of the number and diversity of nations and stakeholders involved in the international supply chain, achieving consensus on these and other standards could be difficult and time consuming.

## Shared Responsibilities Place a Premium on Effective Cooperation

Effective cooperation is essential—and not ensured—even at the domestic level. As we have reported, one challenge to achieving national preparedness and response goals hinges on the federal government's ability to form effective partnerships among many entities.[22] If such partnerships are not in place—and equally important, if they do not work effectively—those who are ultimately in charge cannot gain the resources, expertise, and cooperation of the people who must implement security measures.

Our reviews of domestic seaports have found that such partnerships can break down even when procedures are supposedly in place. For example, at the Port of Honolulu, a security plan exists that calls for notifying the Coast Guard and local law enforcement authorities about serious incidents. One such incident took place in April 2002 when, as cargo was being loaded onto a cruise ship, specially trained dogs reacted to possible explosives in one of the loads, and the identified pallet was set aside. Despite the notification policy, personnel working for the shipping agent and the private company providing security at the dock failed to notify either local law enforcement officials or the Coast Guard about the incident. A few hours after the incident took place, Coast Guard officials conducting a foot patrol found the pallet, and, when told about the dogs' reaction, immediately notified local emergency response agencies. Once again, however, the procedure was less than successful because the various organizations were all using radios that operated on different frequencies, making coordination between agencies much more difficult. Fortunately, the Honolulu incident did not result in any injuries or loss.

[22]U.S. General Accounting Office, *Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success*, GAO-02-899T (Washington D.C.: July 1, 2002); GAO-02-900T (Washington D.C.: July 2, 2002); and GAO-02-901T (Washington D.C.: July 3, 2002).

Just as efforts to enhance port security in the domestic environment require the collaboration of many public and private parties, the challenges internationally require cooperation and collaboration by a wide array of stakeholders. Clearly, there are important initiatives moving forward in the four major international institutions outlined above—on port and carrier standards in the IMO, on customs procedures in the WCO, on seafarer and port worker documentation in the ILO, and on standards for electronic container seals in the ISO. Each organization is made up of individual nations contributing different levels of development, maritime activity, and economic capacity. Admiral James M. Loy, former Commandant of the Coast Guard and current Acting Director of TSA, has emphasized that reaching global agreements is critical, noting that "international and domestic cooperation, both civil and military, is essential…because we can't hope to ensure our security by working alone or by waiting until the threats have already crossed the thresholds of our ports."[23] Although many cooperative efforts are under way to address supply chain security, achieving consensus among the diverse parties on a number of matters in this area and forging comprehensive agreements to address them will be challenging.

## Funding Issues Are Pivotal

Many of the planned security improvements at seaports will require costly outlays for infrastructure, technology, and personnel. Even before September 11th, the Interagency Commission on Crime and Security in U.S. Seaports[24] estimated that the costs for upgrading security infrastructure at U.S. ports will range from $10 million to $50 million per port.[25] Officials at the Port of New York and New Jersey estimate their capital costs for bringing the port's security into compliance with the port's vulnerability assessment at $73 million. The federal government has already stepped in with additional funding for port security, but demand has far outstripped the additional amounts made available.

International ports also may face funding challenges similar to those faced by ports in the United States. Recently, at an Asia Pacific Economic

[23]"The Unique Challenges of Maritime Security," speech by Admiral James M. Loy, Propeller Club of the United States, Washington, D.C., October 31, 2001.

[24]On April 27, 1999, the President established the Interagency Commission on Crime and Security in U.S. Seaports. The Commission issued its report on August 28, 2000.

[25]Estimated range varies on the basis of port size and cost of the technology component of the security upgrade.

Cooperation conference, Secretary of Transportation Norman Y. Mineta echoed this sentiment, saying that implementation of security measures to ensure safety of passengers and goods may challenge the resources of foreign economies. However, the extent of any fiscal challenges faced by specific foreign ports is unknown at this point.

In summary, Mr. Chairman, the nation's approach to dealing with nuclear smuggling is both to develop entirely new lines of defense overseas and to shore up those defenses that are already in place in the nation's ports. The challenges domestically are well known and well chronicled: ports remain susceptible to weapons of mass destruction, with neither our best technology nor a set of clear standards and procedures in place. The challenges overseas could be much the same. Just as inconsistent standards and security vulnerabilities among domestic ports could lead terrorists to seek the path of least resistance, overseas ports that do not adopt strong security standards may attract the attention of those hoping to inflict harm on America. At the domestic level, the challenges faced can be mitigated somewhat by the fact that stakeholders ultimately share the same goals of national security. Although all countries involved in international commerce may share the basic goal of secure trade and may share commitment, foreign countries may vary greatly in their understanding of, vulnerabilities to, and capabilities to address the threats involved.

Mr. Chairman, this completes my prepared statement. I would be pleased to respond to any questions you or other Members of the Subcommittee may have.

## Contacts and Acknowledgments

For information about this testimony, please contact JayEtta Z. Hecker, Director, Physical Infrastructure Issues, at (202) 512-2834. Individuals making key contributions to this testimony include Gene Aloise, Jonathan Bachman, Seto Bagdoyan, Christine Broderick, Steven Calvo, Howard Cott, Laurie E. Ekstrand, Etana Finkler, Gary Jones, Stan Stenersen, Eric Wenner, Randy Williamson, and Loren Yager.

## Scope and Methodology

To determine the programs in place to prevent illegal fissile material or a tactical nuclear weapon from being smuggled into the United States through our ports, we relied on issues raised in a number of GAO-issued products, as indicated in footnote 1.

To determine new efforts under way to improve port and container security, both domestically and abroad, we talked with senior DOT, TSA, and Coast Guard officials, including the Coast Guard representative to the IMO on international initiatives, a senior TSA official regarding the status of rulemaking to govern the Operation Safe Commerce pilot program, and the Deputy Undersecretary of DOT who co-chairs the Container Security Group on international initiatives to advance U.S. recommendations for enhancing port and container security. We also met with representatives from the Ports of Los Angeles, New York and New Jersey, and Seattle—the three ports that are participating in the Operation Safe Commerce pilot program—and discussed the new international and domestic initiatives. We also obtained key documents and "white papers" on initiatives from Coast Guard and DOT officials and from the Coast Guard, Customs, IMO, WCO, ILO, and ISO Internet Web sites.

To determine the key challenges to implementing these initiatives and efforts, we met with senior DOT, TSA, and Coast Guard officials, including the Coast Guard representative to the IMO on international initiatives and the Deputy Undersecretary of DOT who co-chairs the Container Security Group on international initiatives to advance U.S. recommendations for enhancing port and container security. We also met with representatives from the Ports of Los Angeles, New York and New Jersey, and Seattle and discussed the new international and domestic initiatives. We obtained key documents and "white papers" on initiatives from Coast Guard and DOT officials and from the Coast Guard, Customs, IMO, WCO, ILO, and ISO Internet Web sites. We also relied on our previously issued product on port security, GAO-02-993T, August 5, 2002.