TESTIMONY OF

ALAN BERSIN

COMMISSIONER
U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY

BEFORE

SENATE COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE

JULY 21, 2010

Chairman Rockefeller, Ranking Member Hutchison, esteemed members of the Committee, it is a privilege and an honor to appear before you today to discuss U.S. Customs and Border Protection's (CBP) work to secure the flow of goods into and out of the United States—preventing smuggling and protecting the country from dangerous shipments while expediting legitimate commerce. CBP pursues a multilayered approach to security, using a risk management approach that allows us to strategically apply resources to prioritized enforcement objectives and threats.

CBP is at the frontline of protecting the nation from threats, including those posed by containerized cargo. At the core of that mission is preventing chemical, radiological, biological, and nuclear threats, and preventing and disrupting terrorist attacks arising from border crossings. We also stem the illegal flow of drugs, contraband and people, protect our agricultural and economic interests from harmful pests and diseases, protect American businesses from theft of their intellectual property, enforce textile agreements, determine and track import safety violations, regulate and facilitate international trade, collect import duties, facilitate legitimate travel, and enforce U.S. trade laws. In fiscal year 2009, CBP screened 100% of the maritime containers arrived at our seaports through our multilayered approach – 9.8 million in all.

While security is our core mission, CBP also has important trade responsibilities. Our security and trade facilitation missions are mutually supportive: by utilizing risk-based strategies, and applying a multilayered approach, we can focus our time and resources on the small percentage of goods that are high-risk or about which we know the least, which in turn allows us to expedite trade that is low-risk or about which we already know a great deal.

OVERVIEW OF CBP APPROACH

We are operating in the age of integrated global supply chains, and our approach to this environment must be equally comprehensive and global. While inspections and operations at our ports are a key component of our strategy, to fully meet our responsibilities, we must identify and stop threats before they arrive at American ports. This requires that we secure the flow of cargo at each stage of the supply chain—at the point of origin, while in transit, and when it arrives in the United States.

Our multilayered security approach involves:

- Obtaining information about cargo and those involved in moving it early in the process;
- Using advanced targeting techniques to assess risk and building a knowledge base about the people and companies involved in the supply chain;
- Fostering partnerships with the private sector and collaborating with other Federal agencies and departments, such as the U.S. Coast Guard, Department of Health and Human Services, the Consumer Product Safety Commission, Immigration and Customs Enforcement, and the Department of Agriculture, and with foreign governments, including through information sharing;
- Expanding enforcement efforts to points earlier in the supply chain than simply our borders; and
- Maintaining robust inspection regimes, including non-intrusive inspection equipment and radiation detection technologies, at our ports of entry.

We have asked the trade community to assume its fair share of the burden as well, to exercise reasonable care in customs matters, to provide information to better understand the parties to a transaction, and to invest in the resources necessary to keep up with current requirements. CBP strives to provide an environment built upon predictability, transparency, and uniformity in the importing process. We weigh the cumulative costs of our decisions on business and, when possible, provide for simplified commercial processing. CBP and the trade community must be partners, leveraging both parties' expertise.

In addition to addressing security concerns, CBP has also been aggressive in addressing other public safety concerns, such as product safety. CBP has established the Commercial Targeting and Analysis Center (CTAC), which is solely dedicated to import safety concerns. The Import Safety CTAC serves as a fusion center for CBP and other government agencies—including the Consumer Product Safety Commission, the Food and Drug Administration and the Food Safety Inspection Service—to combine resources and manpower to protect the American public from harm that could be caused by unsafe imported products. CBP looks forward to the expansion of this targeting center to include the participation of additional agencies.

With that background, I would like to discuss the operational initiatives that help us fulfill the security, trade and public safety missions I have outlined.

ADVANCE INFORMATION

CBP requires advanced electronic cargo information, as mandated in the Trade Act of 2002 (24-Hour Rule, through regulations), for all inbound shipments in all modes of transportation. CBP requires the electronic transmission of additional data, as mandated by the SAFE Port Act, through the Importer Security Filing and Additional Carrier Requirements rule (Security Filing "10+2"), which became effective as an Interim Final Rule on January 26, 2009, and went into full effect on January 26, 2010. Under the Security Filing "10+2" rule, importers are responsible for supplying CBP with ten trade data elements 24 hours prior to vessel lading, and ocean carriers are required to provide their vessel stow plans no later than 48 hours after

departure and their container status messages no later than 24 hours after creation or receipt. This advance data allows CBP targeting specialists to identify risk factors earlier in the supply chain. Security Filing "10+2" joins the 24 hour rule, and the C-TPAT program and CSI discussed below, in collecting advanced information to improve CBP's targeting efforts.

As part of CBP's layered targeting strategy, the National Targeting Center – Cargo (NTC-C) proactively analyzes advance cargo tactical and strategic information using the Automated Targeting System (ATS) before shipments reach the United States. ATS provides uniform review of cargo shipments for identification of the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. Through targeting rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes of transportation—sea, truck, rail, and air. ATS is a decision support tool for CBP officers working in the NTC-C and in Advanced Targeting Units at our ports of entry and CSI ports abroad.

Once NTC-C has analyzed the advanced information using ATS and other tools, intelligence briefs are created and disseminated to officers in the field. This information is used by CBP and other agencies to support enforcement actions, such as seizures and arrests.

NTC-C has established partnerships and liaisons with other agencies, both domestically and abroad. Partnerships with Immigration and Customs Enforcement, the Drug Enforcement Administration, the Financial Crimes Enforcement Network, the Department of Commerce, and the Department of Health and Human Services promote information sharing and the exchange of best practices, while collaboration with foreign governments results in seizures and detection of threats at our borders and in foreign ports.

CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

CBP works with the trade community through the Customs Trade Partnership Against Terrorism (C-TPAT), a voluntary public–private partnership program wherein some members of the trade community adopt tighter security measures throughout their international supply chain and in return are afforded benefits such as reduced exams, front of line examination privileges to the extent possible and practical, and an assigned Supply Chain Security Specialist who helps them maintain compliance. C-TPAT has enabled CBP to leverage private sector resources to enhance supply chain security.

Prospective C-TPAT members submit basic company information and a security profile through an Internet-based portal system. CBP conducts records checks on the company in its law enforcement and trade databases and ensures the company meets the security criteria for its particular business sector. Members who pass extensive vetting are certified into the program. Using a risk-based approach, CBP Supply Chain Security Specialists conduct on-site visits of foreign and domestic facilities to confirm that the security practices are in place and operational.

C-TPAT has been a success—membership in the program has grown from 7 companies in its first year to 9,897 as of July 8, 2010. C-TPAT's certified partners include 4,416 importers,

2,739 carriers, 843 brokers, 809 consolidators/third party logistic providers, 59 Marine Port Authority and Terminal Operators, and 1,031 foreign manufacturers. C-TPAT has conducted 15,207 onsite validations of manufacturing and logistics facilities in 90 countries. Of those in the program, 313 C-TPAT importer partners have been granted the highest level of program benefits having qualified for Tier 3 status, which means that these companies have exceeded C-TPAT's security requirements.

Additionally, CBP is working with foreign partners to establish bi-national recognition and enforcement of C-TPAT. CBP currently has signed mutual recognition agreements with New Zealand (2007), Canada (2008), Jordan (2008), Japan (2009), and Korea (2010). We are continuing to work towards similar recognition with the European Union and other countries.

CONTAINER SECURITY INITIATIVE

CBP partners with foreign governments through the Container Security Initiative (CSI) to prevent and deter terrorist threats before they reach American ports. CSI enables CBP to identify and inspect high-risk U.S.-bound cargo containers at foreign ports prior to departure. Through CSI, CBP stations multidisciplinary teams of officers to work with host country counterparts to identify and examine containers that are determined to pose a high risk for terrorist activity. CSI, the first program of its kind, was announced in January 2002 and is currently operational in 58 foreign seaports—covering more than 80 percent of the maritime containerized cargo shipped to the United States.

CBP officers stationed at CSI ports, with assistance from CSI targeters at the National Targeting Center–Cargo (NTC–C), review 100 percent of the manifests originating and/or transiting those foreign ports for containers that are destined for the United States. In this way, CBP identifies and examines high risk containerized maritime cargo prior to lading at a foreign port and before shipment to the United States. In FY 2009, CBP officers stationed at CSI ports reviewed over 9 million bills of lading and conducted over 56,000 exams in conjunction with their host country counterparts.

As the CSI program has matured, CBP looked for opportunities to increase efficiencies and reduce costs by shifting functions to the NTC–C. CBP's ability to target high risk containers has progressed to the point that much of the work can be done from CBP's U.S. location rather than through a physical presence overseas. CBP is exploring opportunities to utilize emerging technology in some locations, which will allow the program to become more efficient and less costly. In January 2009, CBP began to reduce the number of personnel stationed overseas who perform targeting functions, increasingly shifting the targeting of high risk containers to personnel stationed at the NTC–C. This shift in operations reduces costs without diminishing the effectiveness of the CSI program. CBP will remain operational in all 58 locations in fiscal year 2011 with sufficient personnel in country to conduct the examinations of high risk shipments with the host government and to maintain relationships with their host-country counterparts.

SECURE FREIGHT INITIATIVE

The Secure Freight Initiative (SFI) is an effort to enhance the U.S. government's ability to scan containers for nuclear and radiological materials at seaports worldwide and better assess the risk of inbound containers. This initiative is the culmination of our work with other Federal agencies, foreign governments, the trade community, and vendors of cutting-edge technology. SFI provides carriers of maritime containerized cargo greater confidence in the security of the shipment they are transporting, and increases the likelihood of an uninterrupted and secure flow of commerce.

In advancing the goal of 100% scanning, the Secure Freight Initiative (SFI) deploys networks of radiation detection, provided by the Department of Energy, our partner in SFI, and imaging equipments at five overseas pilot ports. This advanced pilot has encountered a number of serious challenges to implementing the 100% scanning mandate.

Certain challenges are logistical. Many ports simply do not have one area through which all the cargo passes; there are multiple points of entry, and cargo is "transshipped," meaning it is moved immediately from vessel to vessel within the port. These ports are not configured to put in place detection equipment or to provide space for secondary inspections. At these ports, scanning 100% of cargo with current systems is currently unworkable without seriously hindering the flow of shipments or redesigning the ports themselves, which would require huge capital investment.

Other challenges are the limitations that are inherent in available technology. DHS currently uses both passive radiation detection and active x-ray scanning to look for radioactive material in cargo. An important obstacle is the absence of x-ray scanning technology which can effectively and automatically detect suspicious anomalies within cargo containers that should trigger additional inspection. Currently, DHS personnel visually inspect screens for possible anomalies, but the scale and the variety of container cargo make this process challenging and time-consuming. In addition, current x-ray systems have limited penetration capability; this can limit their ability to find a device in very dense cargo.

While DHS is pursuing technological solutions to these problems, expanding screening with available technology would slow the flow of commerce and drive up costs to consumers without bringing significant security benefits.

Finally, and on that note, the costs of 100% scanning pose a great challenge, particularly in a struggling economy. Deploying SFI-type scanning equipment would cost about $8 million per lane for the more than 2,100 shipping lanes at more than 700 ports around the world that ship to the United States. On top of these initial costs, operating costs would be very high. These include only DHS expenses, not the huge costs that would have to be borne by foreign governments or industry. It is also important to keep in mind that about 86% of the cargo shipped to the United States is sent from only 58 of those more than 700 ports. Installing equipment and placing personnel at all of these ports – even the tiny ones – would strain government resources without a guarantee of results.

Thus, in order to implement the 100% scanning requirement by the 2012 deadline, DHS would need significant resources for greater manpower and technology, technologies that do not

currently exist, and the redesign of many ports. As Secretary Napolitano has indicated, these are all prohibitive challenges that will require the Department to seek the time extensions authorized by law.

NON INTRUSIVE INSPECTION / RADIATION DETECTION TECHNOLOGY

The deployment of imaging systems and radiation detection equipment has made a tremendous contribution to CBP's progress in securing the supply chains that bring goods into the United States from around the world against exploitation by terrorist groups. Non-Intrusive Inspection (NII) technology serves as a force multiplier that allows officers to detect possible anomalies between the contents of a container and the manifest. CBP's use of NII allows us to work smarter and more efficiently in recognizing potential threats.

CBP has aggressively deployed NII and RPM technology. Prior to 9/11, not a single Radiation Portal Monitor (RPM), and only 64 large-scale NII systems, were deployed to our country's borders. Today, CBP uses RPMs to scan 99 percent of all cargo arriving in the U.S. by land and sea. CBP, in partnership with the DHS Domestic Nuclear Detection Office (DNDO) and Pacific Northwest National Laboratory (PNNL), has deployed 493 RPMs at northern border land ports of entry; 392 RPMs at southern border land ports of entry; 451 RPMs at seaports; and 52 RPMs at mail facilities. Currently, CBP has 267 large-scale NII systems deployed. Additionally, CBP has deployed over 1,700 Radiation Isotope Identifier Devices (RIIDs) and over 20,000 Personal Radiation Detectors (PRDs). These devices allow CBP to examine 100 percent of all identified high-risk cargo. To date, CBP has used the deployed NII systems to conduct over 42 million examinations, resulting in over 8,300 narcotic seizures, with a total weight of over 2.6 million pounds, and over $28.6 million in undeclared currency seizures. Since RPM program inception in 2002, CBP has scanned over 438 million conveyances for radiological contraband, resulting in over 2.7 million alarms. CBP's Laboratories and Scientific Services 24/7 Teleforensic Center spectroscopy group at the National Targeting Center has responded to over 23,000 requests from the field for technical assistance in resolving alarms. To date, 100 percent of alarms have been successfully adjudicated as innocent, legitimate trade, legitimate transportation, or non-terrorism related.

CONCLUSION

Mr. Chairman, Members of the Committee, thank you again for this opportunity to testify about CBP's commitment to enhancing cargo security. We look forward to continuing to work with the Committee on this issue. I will be happy to answer any of your questions.