Acting Commissioner Ahern Testifies on Strengthening the Security of Containerized Cargo
(04/01/2009)

Statement of Jayson P. Ahern, Acting Commissioner,
U.S. Customs and Border Protection,
Department of Homeland Security before the Committee on Appropriations, Subcommittee on Homeland Security.

Introduction

Chairman Price, Ranking Member Rogers, distinguished Members of the Subcommittee, it is a privilege and an honor to appear before you today to discuss the work of U.S. Customs and Border Protection (CBP) to both strengthen the security of containerized cargo entering our borders and facilitate the flow of legitimate trade and travel.

Let me begin by expressing my gratitude to the Committee for the strong support you provided for important initiatives implemented by CBP last year. Your support has enabled CBP to make significant progress in securing our borders and protecting our nation against the terrorist threat. CBP looks forward to working with you to build on these successes.

I would also like to thank you for your support in the Economic Stimulus bill. The American Recovery and Reinvestment Act of 2009 provided $680 million to CBP for greatly needed investment in our aging infrastructure. These funds will support planning, management, design, alteration, and construction of CBP-owned land ports of entry; procurement and deployment of non-intrusive inspection system; expedited development and deployment of border security technology on the southwest border; and for the procurement and deployment of tactical communications equipment. In addition, the bill also included $300 million for the construction and repair of land ports of entry owned by the General Services Administration (GSA). We are moving swiftly to put these investments to good use.

CBP is the largest uniformed, federal law enforcement agency in the country. We station over 20,000 CBP officers at access points around the nation – air, land, and sea ports. By the end of FY 2009, we will have deployed over 20,000 Border Patrol agents between the ports of entry. These forces are supplemented with 980 Air and Marine agents, 2,260 agricultural specialists, and other professionals.

I am pleased to report that CBP continues to achieve success in performing our mission, which include stemming the flow of illegal drugs and contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, enforcing violations of textile agreements, tracking import safety violations, protecting the economy from monopolistic practices, regulating and facilitating international trade, collecting import duties, and enforcing United States trade laws. At the same time, our employees maintain a vigilant watch for terrorist threats. In FY 2008, CBP processed more than 396 million pedestrians and passengers, 122 million conveyances, 29 million trade entries, collected $32.5 billion in revenue, examined 5.6 million sea, rail, and truck containers, performed over 25 million agriculture inspections, apprehended over 720 thousand illegal aliens between our ports of entry, encountered over 220 thousand inadmissible aliens at the ports of entry, and seized more than 2.8 million pounds of narcotics.

I want to begin by expressing my gratitude to the Committee for the interest and support you continue to provide as CBP performs our important security and trade enforcement work without stifling the flow of legitimate trade and travel that is so important to our nation's economy. We continue to refine a risk-based and layered approach to accomplish our "twin goals:" building more secure and more efficient borders that at the same time will facilitate legitimate trade and travel.

Mr. Chairman, once the CBP Fiscal Year 2010 budget request is submitted to Congress, I would be more than happy to discuss our request with you and your staff. We appreciate your strong support in previous years and look forward to working with this committee over the next year.

CBP Overview

I am pleased to appear before the Subcommittee today to highlight key accomplishments related to container security. Since the last time I testified, CBP has continued to make tremendous progress in ensuring the supply chains that bring goods into the United States from around the world are more secure against potential exploitation by terrorist groups as a means to deliver weapons of mass effect.

CBP uses a multi-layered approach to ensure the integrity of the supply chain from the point of stuffing through arrival at a U.S. port of entry. This multi-layered approach includes:

- Advanced information under the 24-Hour Rule and Trade Act of 2002 (supplemented now by our Importer Security Filing requirements)
- Screening the information through the Automated Targeting System (ATS) and National Targeting Center – Cargo (NTC-C)
- Partnerships with industry and the private sector such as the Customs Trade Partnership Against Terrorism (C-TPAT)
- Partnerships with foreign governments, such as the Container Security Initiative (CSI) and the Secure Freight Initiative (SFI)
- Use of Non-Intrusive Inspection (NII) technology and mandatory exams for all high risk shipments

The goal of this layered approach is to combine each of these systems to allow us to receive, process, and act upon commercial information in a timely manner so that we can target, in a very specific fashion, the suspect shipments without hindering the movement of commerce through our ports.

While I will discuss each one of these layers in greater detail, I would first like to clarify a few points with respect to our multi-layered approach. Different layers focus on securing different parts of the supply chain, ensuring that cargo is regularly assessed and that security does not rely on any single point that could be compromised. Our approach is to look at all of these distinct but related threats and rely upon a layered security process which is designed to reduce risk to the extent possible.

We are continuously working to refine this layered process; our efforts focus on strengthening our tools and capabilities while at the same time maintaining an appropriate balance that considers the wide range of threats and allocates our limited resources accordingly. My concern, however, is that the continuous focus on certain areas is often maintained at the expense of other, equally important areas that require similar attention.

For example, DHS has dedicated significant resources and efforts to our cargo and port security programs over the last several years, resulting in a robust risk-management approach. Our focus on risk management and security has to be driven by our informed judgment about the totality of risks. We must

also remain focused on other threats to our ports and to other components of the supply chain. For example, we must remain vigilant in securing all conveyances and screening passengers at our land borders, airports, railways, and small vessels terminals.

In order to manage risk for all arriving cargo and passengers, we must direct our resources to those areas which represent the greatest threat. While the maritime environment does contain some element of risk for a weapon of mass effect to be transported in a maritime container, the logistics movements which involve multiple hand offs amongst various parties throughout the supply chain may in fact itself be a deterrent to a terrorist considering using a maritime container. In addition, as outlined in my testimony, much has been done to enhance the security of maritime containers and cargo compared to some other areas. As the Department and the Congress look to apply limited resources to multiple areas of threat and vulnerability, we should therefore not over emphasize maritime containers at the potential detriment of other threat areas in need of resources.

I would like to discuss each one of these layers in greater detail.

Advance Information

CBP has recognized Congress' mandate that we collect more and improved advanced information for cargo shipments. CBP, in fact, requires advanced electronic cargo information as mandated in the Trade Act of 2002 (including the 24-Hour Rule for maritime cargo). Advanced cargo information on all inbound shipments for all modes of transportation is evaluated through the Automated Targeting System (ATS) before arrival in the United States.

The function of ATS is to provide information to support the decisions of CBP officers working in Advance Targeting Units (ATUs) at our ports of entry and CSI ports. The system provides a uniform review of cargo shipments, identifies the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. ATS uses a rules-based program to highlight potential risk, patterns, and targets. Through rules, ATS alerts the user to data that meets or exceeds certain predefined criteria. ATS uses national targeting rule sets to provide threshold targeting for national security risks for all modes: sea, truck, rail, and air. CBP is continually striving to improve the ATS system by convening regular "rules conferences". The conferences are attended by our intelligence officers and representatives from various seaports and land border ports who update risk indicators and ensure that the most current intelligence and trends are factored into ATS.

CBP has been working with importers for several years to put in place a rule that would ensure that we had timely access to the information necessary to perform a proper analysis of the risk posed by particular shipments. After that effort began, Congress endorsed it-- the SAFE Port Act mandated that CBP obtain additional advanced cargo information to enhance our ability to perform risk-based targeting prior to cargo being laden on a vessel overseas.

As many of you know, CBP announced an Interim Final Rule (IRF) in January 2009 that requires importers and carriers to electronically submit additional information on cargo before it is brought into the United States by vessel. Since then, CBP has received tens of thousands of Importer Security Filing (ISF) filings, hundreds of vessel stow plans and millions of container status messages that have already yielded some promising results.

The additional data elements that DHS is receiving under the importer security filing rule are critical to ensuring that we have the best information available about where a container originated, who filled it with goods, where this may have occurred, and what types of goods are being shipped.

The trade's input during the consultative process as well as its participation in the Advance Trade Data Initiative was instrumental in the successful crafting of the rule. CBP made several significant changes to the proposed rule based on feedback received during its consultation with industry partners, the Departmental Advisory Committee on Commercial Operations (COAC), and other federal entities.

These changes include a year-long delayed compliance period, considerable flexibilities associated with six of the data requirements, and a commitment to accept additional comments from industry until June 1, 2009 and then initiate a structured review to reexamine the rule's impact on industry. Based upon this review, DHS will determine whether to eliminate, modify, or maintain these requirements.

The CBP Importer Security Filing covers the following key areas:

1. Ten unique data elements from importers not currently provided to CBP 24 hours prior to foreign loading of cargo
    - Manufacturer (or supplier) name and address
    - Seller (or owner) name and address
    - Buyer (or owner) name and address
    - Ship to name and address
    - Container stuffing location
    - Consolidator (stuffer) name and address
    - Importer of record number/foreign trade zone applicant identification number
    - Consignee number(s)
    - Country of origin
    - Commodity Harmonized Tariff Schedule of the United States number
2. Two additional data elements provided by the carriers, including the Vessel Stow Plan, which is currently utilized by the vessel industry to load and discharge containers, and Container Status Messaging, which is currently utilized by the vessel industry to track the location of containers and provide status notifications to shippers, consignees and other related parties.

Customs Trade Partnership Against Terrorism (C-TPAT)

C-TPAT is an integral part of the CBP multi-layered strategy through which CBP works in partnership with the trade community to better secure goods moving through the international supply chain. C-TPAT has enabled CBP to leverage supply chain security throughout international locations where CBP has limited regulatory reach.

In FY 2009, C-TPAT will focus its efforts on strengthening the partnership with member companies at both the macro and micro levels and leverageing corporate influence throughout the international supply chain. In doing so, C- TPAT will continue to ensure compliance with the requirements of the SAFE Port Act to include certifying security profiles within 90 days of submission and conducting validations within 1 year of certification and revalidations within 4-years of initial validation. C-TPAT projects that 3,200 validations will be required during FY 2009, requiring on site visits at facilities throughout the world.

In strengthening this successful program, CBP will also continue to review its performance and, where needed, enhance the minimum security criteria for each enrollment sector. Additionally, CBP will continue to conduct informational and training sessions for various internal / external audiences to improve knowledge of cargo security procedures and provide the latest information regarding terrorism trends and conveyance breeches.

In exchange for adopting these stronger security practices, CBP affords companies that participate in C-TPAT a range of benefits associated with the facilitation of their goods through the security processes at the border. These benefits include: cost and delay savings associated with reduced examinations, expedited treatment when examinations are warranted, tighter inventory control of assets, business resumption privileges, ability to supply goods or services to those U.S. importers who require suppliers to have acceptable supply chain security programs, and a competitive advantage over firms with no or limited supply chain security programs. For example, under the current program, C-TPAT membership often results in reduced security inspections; C-TPAT importers are 6 times less likely to incur a security examination and 4 times less likely to incur a compliance examination.

Another important effort to note is the potential mutual recognition of other countries' customs-to-business partnership programs. The World Customs Organization has developed a global standard for trusted partnerships with the trade, known as the Authorized Economic Operator, or AEO, program. This concept is similar to our C-TPAT. Mutual Recognition Arrangements reduce costs and simplify these programs for both industry and government.

Creating an international network to exchange information about trusted traders and knowing that those participants are observing specified security standards in the secure handling of goods and relevant information is a win-win for both government and business. In 2007, CBP signed its first mutual recognition arrangement with New Zealand, and in 2008, additional mutual recognition agreements were signed with Canada and Jordan. We are beginning to see several positive outcomes and challenges taking form as the work to implement these arrangements continue.

Container Security Initiative (CSI)

To further our priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP has partnered with other countries through our Container Security Initiative (CSI). Almost 32,000 seagoing containers arrive and are off loaded at United States seaports each day and under CSI, which is the first program of its kind, CBP partners with foreign governments to screen containers at foreign ports and then identify and inspect high-risk cargo containers at those foreign ports, before they are shipped to our seaports and pose a threat to the United States and to global trade.

The goal is for CBP's overseas CSI teams to review all the manifests before containers are loaded on vessels destined for the United States. However, in those locations where the CSI team cannot review all the bills because of the tremendous volume, CSI targeters at the National Targeting Center - Cargo provide additional support to ensure that 100 percent review is accomplished. Utilizing the overseas CSI team and the CSI targeters at our National Targeting Center - Cargo, CBP reviews 100 percent of manifests under the CSI program.

Oversight of the CSI program is supported by automated tools for statistical analysis, an evaluation database to track and analyze any deficiencies identified during the evaluation process of the CSI ports, and a non-intrusive inspection (NII) equipment utilization database that tracks the use of NII equipment at CSI ports to include the downtime of the equipment.

Today, CSI has partnered with 32 countries and is operational in 58 ports world-wide, and over 86 percent of the containerized maritime cargo destined for the United States originates or passes through a CSI port. In FY 2008, 95 percent of the examinations requested from our host government partners were performed – over 74,000 examinations – bringing greater security and trade facilitation within the international supply chain.

Secure Freight Initiative (SFI)

The Secure Freight Initiative (SFI) pilot scanning project is another component of this layered enforcement strategy for protecting the nation. Integrated scanning systems, consisting of Radiation Portal Monitors (RPMs) provided by DOE/NNSA and NII imaging systems provided by CBP or the host nation, are used to scan containers as they move through the foreign ports. Data from these systems is integrated utilizing optical character recognition (OCR) technology and provided to CBP officers who determine if the container should be referred to the host nation for secondary examination prior to lading.

Meeting the legislative requirements of the SAFE Port Act, the first three SFI pilot ports (Puerto Cortes, Honduras; Port Qasim, Pakistan; and Southampton, United Kingdom) became fully operational on October 12, 2007, and are attempting to scan 100 percent of U.S.-bound maritime containers (total U.S.-bound container volume at these three ports from October 12, 2007 to March 11, 2009 was 255,424). Furthermore, CBP and DOE expanded the deployment of scanning equipment to one terminal in Hong Kong, recently began operations in Port Busan (South Korea), and will soon be operational in Salalah (Oman). CBP has also been working very closely with Pakistan Customs to expand the SFI model to Karachi, and we are hopeful that we can begin scanning containers from Karachi later this year.

SFI chose these initial ports because they present a unique set of challenges and provide diverse environments in which to evaluate varying options. While these are the deployments currently planned and anticipated, we are constantly assessing the priority of foreign ports and terminals that present the greatest opportunities to reduce risk through deployment of SFI resources and will adjust our deployment plans and schedule accordingly and keep the Committee informed.

Multiple reports have been submitted to Congress since October 2007, which outline the lessons learned through SFI, and another report will be sent to Congress later this month. The lessons learned from the SFI deployments in Pakistan, Honduras, Southampton and Hong Kong demonstrate that scanning U.S.-bound maritime containers is possible on a limited scale, focusing primarily on gate traffic (there is currently no proven technology which can address transshipped containers), however, results are based on scanning on a very limited scale. Scanning all 11.3 million containers that enter U.S. seaports from a foreign port presents significant operational, technical, and diplomatic challenges. They include:

- Sustainability of the scanning equipment in extreme weather conditions and certain port environments
- Varying and significant costs of transferring the data back to the United States (National Targeting Center) in real-time
- Re-configuring port layouts to accommodate the equipment without affecting port efficiency and getting the permission of host governments
- Developing local response protocols for adjudicating alarms
- Addressing health and safety concerns of host governments and local trucking and labor unions
- Identifying who will incur the costs for operating and maintaining the scanning equipment
- Acquiring necessary trade data prior to processing containers through the SFI system
- Addressing data privacy concerns in regards to the scanning data
- Concluding agreements with partnering nations and terminal operators to document roles and responsibilities regarding issues such as ownership, operation, and maintenance of the equipment; sharing of information; and import duty and tax considerations
- Staffing implications for both the foreign customs service and terminal operator
- Licensing requirements for the scanning technology
- Host government support for continuing to scan 100 percent of U.S. bound containers after the pilot ends

- The potential requirements for reciprocal scanning of U.S. exports

DHS supports the general goal of expanding scanning abroad and is now working to address these challenges in a manner consistent with the risk-management and layered approach to maritime cargo security we have in place and in a manner consistent with the World Customs Organization (WCO) SAFE framework of standards.

While we work to address the complex challenges we have encountered, the focus now is on determining how to achieve efficient expansion while maximizing the security benefit and containing the cost. As Secretary Napolitano indicated in her recent testimony, achieving 100 percent scanning by 2012 will be difficult based on what we know today. CBP is currently taking a close look at what will be possible and useful and will come back to the Congress soon with a clear path forward.

Non-Intrusive Inspection (NII) and Radiation Detection Technology

Technologies deployed to our nation's sea, air, and land border ports of entry include non-intrusive imaging equipment, such as large-scale X-ray and gamma-imaging systems, as well as a variety of portable and hand-held technologies to include radiation detection technology. NII technologies play a key role in CBP's layered strategy and are viewed as force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic quickly, while facilitating the flow of legitimate trade, cargo, and passengers. Presently, CBP deploys 223 large scale cargo inspection systems to our ports of entry, 87 of which are in seaports.

An integral part of CBP's comprehensive strategy to combat nuclear and radiological terrorism is to scan all arriving sea containers with radiation detection equipment prior to release at domestic ports. Currently, CBP has 409 Radiation Portal Monitors (RPM) deployed at priority seaports in the United States, through which approximately 98 percent of all arriving sea-borne containerized cargo passes. CBP is forecasting the deployment of 83 additional seaport RPMs by the end of FY 2009.

Additionally, we currently have 335 RPMs on the northern border, which provides CBP with the capability to scan 96 percent of truck cargo and 88 percent of personal owned vehicles (POVs) for illicit radiological/nuclear materials. The current forecast calls for the deployment of an additional 291 northern border RPMs. This will give CBP the capability to scan approximately 100 percent of truck cargo and 100 percent of personal vehicles for illicit radiological/nuclear materials with RPMs. CBP will also increase the southern border RPM deployments (currently scanning 100 percent of all truck cargo and 95 percent of POVs). By the end of FY2009, CBP plans to deploy 46 additional southern border RPMs - providing CBP with the capability to scan approximately 100 percent of POVs.

In the meantime, CBP, in partnership with the Domestic Nuclear Detection Office (DNDO), is continuing to move forward with the testing and evaluation of the next-generation RPMs, known as Advanced Spectroscopic Portals (ASP). The goal of ASP development is to further improve the efficiency of radiological scanning of cargo containers.

Role of Technology

I would like to take just a moment to discuss the role of technology for supply chain security. Security technology is continuously evolving, not only in terms of capability but also in terms of compatibility, standardization, and integration with information systems. It is important to note that there is no single technology solution to improving supply chain security. As technology matures, it must be evaluated and adjustments to operational plans must be made. Priority should be given to effective security solutions

that complement and improve the business processes already in place, and which build a foundation for 21st century global trade. A more secure supply chain also can be a more efficient supply chain.

Both the SAFE Port Act of 2006 (SAFE Port Act) and the Implementing Recommendations of 9/11 Act of 2007 (9/11 Act) reference the potential benefits of container security standards and devices (CSDs) and encourage DHS to move forward with their development and implementation. However, neither law prescribes a clear path for their development and use. The SAFE Port Act provided the Secretary of DHS with the authority to initiate a rulemaking process and issue an interim rule to establish minimum standards and procedures for security containers in transit to the United States. The provision established that if the rule was not issued, the Secretary would submit a letter of explanation to Congress.

Because DHS does not believe that, at the present time, the necessary technology exists to adequately improve container security without significantly disrupting the flow of commerce, the Department did not make use of the rule-making authority or mandate the use of CSDs and instead issued the required congressional notification letter on May 18, 2007. DHS thereby fulfilled the requirements under this provision of the SAFE Port Act.

The 9/11 Act amended the SAFE Port Act by establishing that if an interim final rule was not issued by the Secretary of DHS by April 1, 2008, all containers in transit to the U.S. would be required to be secured with a seal meeting the International Standards Organization Publicly Available Standard (ISO PAS) 17712, Freight Containers – Mechanical Seals, by October 15, 2008. This specification addresses seal strength and durability so as to prevent accidental breakage or early deterioration, detect tampering, and mark each seal clearly and legibly with a unique identification number. DHS chose to implement this seal mandate, and since October 15, 2008 all containers entering the U.S. are required to be secured with a seal meeting ISO PAS 17712. Our officers in our seaports report a very high level of compliance with this requirement.

It is important to note that CSD technology only improves container security if one can ensure the integrity of the shipment before the CSD is activated. Requiring such a device independent of a process to ensure that the goods within a container were secure before its application would have an adverse effect on security, creating the false impression that a dangerous shipment was secure.

While DHS has decided to not exercise its rule-making authority regarding CSDs to-date, we continue to explore the potential efficiency of these technologies and how they can best enhance container security in very specific trade lanes. In December 2007, CBP issued a Request for Information (RFI) to monitor the state of technology and to acquire and test the most promising commercial-off-the-shelf (COTS) solutions for container security and in-bond shipments. CBP contacted the three most promising technology vendors, yet only one was able to deliver devices for testing. Even though this vendor's system did not fully meet published CBP requirements, CBP decided to proceed with laboratory, then operational field testing. Operational field testing was scheduled to commence in January 2009; however, the vendor made an internal decision to terminate their participation thus eliminating the most promising CSD contender. As a result, there is no CSD system currently available that meets the published requirements, which were developed to reflect CBP's operational needs. On March 5, 2009, CBP submitted a full report to this subcommittee on CBP's progress to date on conveyance security devices and their use in the global supply chain.

In parallel with the evaluation of COTS CSD systems, the U.S. Department of Homeland Security (DHS)'s Science & Technology Directorate (S&T) has been working on developing CSD and Advanced CSD systems. CBP has been coordinating with DHS S&T to monitor the progress of these developmental activities and plans to conduct testing when devices become available.

Conclusion

Mr. Chairman and members of the Subcommittee, your continued support of CBP has led to many positive outcomes in container security. These investments are paying off each day and the recent investments in CBP's aging infrastructure will soon be evident. The resources we put at our border, whether it's people, technology, or tactical infrastructure enhance our ability to address all hazards and all threats at our nation's borders.

Thank you for the opportunity to testify today. I will be happy to answer any questions you may have.