Department of Homeland Security

Statement of
Stewart Baker

Assistant Secretary, Policy

Hearing before the
Committee on Homeland Security and Governmental Affairs
U. S. Senate

October 16, 2007

One Year Later: A Progress Report on the SAFE Port Act

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, I would like to thank you for the opportunity to speak today about the progress we have made improving port and maritime cargo security since the passage of the Security and Accountability For Every Port Act (SAFE Port Act).

This hearing, coming only a few days after the one-year anniversary of the enactment of the SAFE Port Act, provides an opportunity to discuss not only the Department of Homeland Security's (DHS) implementation of the Act's requirements, but also to reflect on the reasons behind our continued efforts.

As many Members of this committee are aware, approximately 32,000 seagoing containers arrive and are off- loaded at United States seaports each day. In fiscal year 2006, that equated to 11.6 million cargo containers.

To put this in a visual context, the National Mall – from the steps of the Capitol to the Washington Monument - could hold a single layer of just 13,068 containers (twenty foot equivalent units). If you wanted to put all the containers that arrive in the United States annually on the National Mall, you would have 13,068 stacks that were each 888 containers high.

These figures illustrate the incredible volume of maritime containerized cargo transiting the global supply chain. Because so much of the world's trade converges in the maritime supply chain, it is uniquely vulnerable to terrorist exploitation. An efficient maritime transportation system is vital to the global economy, but it can also be used to move dangerous cargo to our ports and cities. Simply put, we are talking about a vital global supply chain that serves a vibrant, interdependent global economy – and the importance of protecting it.

The SAFE Port Act displays a broad, strategic vision, covering more than 75 different sections, and touching on all aspects of the existing maritime security architecture -- from securing the containers that transit the supply chain, to defending the vessels and ports that connect it, to ensuring the protection and accountability of the people that work within it.

This noteworthy legislation, with its broad support, reflects the close collaboration between DHS and both the House and the Senate during its development. The SAFE Port Act recognizes the importance of balancing the security of America's borders with the necessity of facilitating legitimate trade and travel. The Act recognizes that any disruptions to this maritime transportation system will have immediate and lasting consequences for our economy and the world at large.

The DHS approach to SAFE Port Act

DHS commends the work of this Committee in addressing the vulnerabilities of containerized cargo through this legislation and through the continued dialogue we have had as we work to implement the Act's many provisions. We appreciate the Committee's

recognition of a number of notable DHS successes through the codification of initiatives and programs that DHS undertook immediately after the 9/11 terrorist attacks and has been implementing successfully ever since.

The SAFE Port Act directs DHS to complete more than 100 specific tasks – an ambitious undertaking. We have completed over 50 to-date and are on track for the remaining provisions. Simply put, the overwhelming majority of requirements mandated by the SAFE Port Act have either been completed or are on schedule to be completed within the required timeframe.

One of the Department's most ambitious achievements over the last year has been the fulfillment of the Act's foreign scanning pilot program requirement, under the Secure Freight Initiative (SFI). SFI became fully operational on October 13th in three foreign ports: Qasim (Pakistan), Cortes (Honduras), and Southampton (United Kingdom). All maritime containerized cargo destined for the U.S. from these locations is currently being scanned and that information is being analyzed by U.S. Customs and Border Protection (CBP) officials stationed in-country and domestically and is available to the host nation government.

Other significant SAFE Port Act accomplishments include:

- On October 3 of this year, USCG published the proposed rule for the Long Range Identification and Tracking (LRIT), which will facilitate the Government's use of the full range of classified and unclassified vessel tracking information available.
- USGC has increased the pace of foreign port assessments, is on track to complete an initial assessment of all of our trading partners by March 2008, and anticipates conducting assessments on a two year cycle thereafter.
- The final Transportation Worker Identification Credential (TWIC) joint rule was published on time by the Transportation Security Administration (TSA) and the USCG. The rule establishes standards and procedures for gaining unescorted access to the Nation's ports and vessels.
- The International Strategy to Enhance Supply Chain Security was also released on time and received input from both the National Maritime Security Advisory Council (NMSAC) and the Commercial Operations Advisory Committee (COAC).
- The Cargo, Maritime, and Trade Office (CMT) was established within the Policy Directorate to coordinate all cargo security programs among the various agencies and departments, as well as effectively engage all relevant stakeholders, including the private sector, in the development of policies and regulations.
- CBP is on track to screen approximately 98 percent of all sea-borne containerized cargo entering the United States for illicit radiological/nuclear materials with radiation portal monitors by the end of December 31, 2007.

Overall, DHS has been working aggressively, and often within constrained timeframes, toward the full implementation of the Act's requirements. While much has been accomplished, there remain a few mandates we have yet to achieve. The remaining requirements are either very close to completion or face outstanding technological

challenges, which have required DHS to seek alternative solutions, and in some cases, reach out to our international and industry partners.

In reflecting on the not yet completed mandates, two themes emerge that often explain the limits we face as we work to translate written words in the Act into meaningful and successful programs. The first theme is that programs built on new technology need to proceed carefully and meticulously. The second theme is that because the supply chain extends across the entire globe, securing it requires close cooperation and partnerships with our foreign counterparts. Neither technological development nor diplomacy reacts well to being rushed. Small delays early on pay dividends and result in stronger, more effective programs in the long run.

The Pace of Technology

I would like to expand on the first theme – the tension between the pace of technology development and how it shapes the rate of policy implementation. The right technological advancements can augment security dramatically: technology can act as a force multiplier, a tool for organizing and sifting through mammoth amounts of data, and can expand the speed and breadth of communications. However energized we are about achieving the benefits of technology now, the brutal reality is that sometimes the pace of technological development does not accord with the policy deadlines we seek to achieve.

The SAFE Port Act addresses many cases in which new technological tools have the potential to greatly increase security. Sometimes, these technologies are ready for use and can provide immediate benefits. This is the case with the non-intrusive inspection (NII) technologies that we deploy at domestic ports of entry to obtain images of the contents of containers. These NII technologies help our Customs and Border Protection officers every day to identify threats, contraband and other anomalies as goods enter our ports.

However, often, the process of transitioning technology from the factory where it is designed or the laboratory where it is tested, into the operational realm can be challenging. We face this challenge as we seek to implement: 1) the Transportation Worker Identification Credential program, 2) the overseas radiological and nuclear scanning pilot, and 3) as we consider means to secure containers using new technologies.

Transportation Worker Identification Credential (TWIC)
The Transportation Worker Identification Credential program offers an example of new technology that will quickly confirm a port worker's identity. TWIC is one of the world's most advanced, interoperable biometric credentialing programs. When it is ready, the new card reader technology that can verify an encrypted biometric will augment the security of our nation's ports.

In order to successfully achieve this vision, the TWIC program is moving towards its objectives, making decisions focused on enhancing port security through a reasoned, phased-in implementation.

TSA is also moving forward on the pilot program called for in the Act to test the TWIC biometric card readers and has identified the Port Authorities of Los Angeles; Long Beach; Brownsville, Texas; and New York and New Jersey; as well as Watermark Cruises of Annapolis, Maryland as pilot participants.

While it has unfortunately proved impossible to meet every SAFE Port Act deadline for TWIC, I am confident that the hard work and time the Department is putting into technology and requirements development, incorporating Congressional and industry input, and developing a careful deployment approach will result in a stronger, healthier and more efficient TWIC program that will protect our country's ports into the future.

Secure Freight – Overseas Scanning Pilot
As I mentioned earlier, the overseas scanning pilot called for in the Act is now operational in three foreign ports, meeting the SAFE Port deadline. This pilot is the first part of our Secure Freight Initiative. Under SFI, DHS and our partner, the Department of Energy, have deployed non-intrusive imaging, radiation detection equipment, and optical character recognition technology abroad to provide an integrated scan of U.S.-bound container cargo. Information from this technology, combined with our normal analysis of manifest data, will provide a comprehensive, real-time approach to assessing the risk of every container bound for the United States.

The process has not been simple; integrating radiation portal monitors, non-intrusive inspection equipment, and optical character readers into each port has presented serious challenges. For instance, successfully deploying the container scanning equipment has required re-configuring certain port layouts to accommodate the equipment without adversely affecting port efficiency. Additionally, some equipment functions differently in extreme weather conditions. Different countries have varying degrees of existing information technology (IT) infrastructure, and the costs of transferring the data back to the United States (to the National Targeting Center) in real-time can be very high. However, in Port Qasim (Pakistan), Puerto Cortes (Honduras), and the Port of Southampton (United Kingdom), we continue to work successfully with our partners at the Department of Energy, our international allies, and industry to address these issues daily.

The department's next step is to expand the program, in a limited capacity, to four more ports in Hong Kong, Salalah (Oman), Port Busan (South Korea), and Singapore. DHS chose to partner with these ports because they pose different challenges and provide diverse environments in which to evaluate various technology options. Hong Kong, Busan and Singapore are three of the world's largest ports and different space constraints and speed of traffic in each present challenges that must be overcome for scanning to work effectively. Salalah has a very high rate of transshipped traffic that enters the port via ship and does not travel through the port's gates, where the scanning equipment is traditionally placed. Each of these ports will offer vital lessons and evidence on how this

integrated suite of scanning technology can meld smoothly into the logistics, operations, and flow of commerce at different ports.

The Department will prepare and submit a report to Congress in April 2008, as mandated in the SAFE Port Act, detailing the progress made in these first seven Secure Freight Initiative ports. The report will outline the successes and challenges we have faced while implementing scanning in foreign locations, including: the availability, capabilities and efficiency of technology and equipment; the process of negotiations with our host nation counterparts as well as their input and feedback on the scanning in their ports; the impact on the movement of cargo through ports and across the global supply chain; the staffing and human capital requirements that will be necessary both abroad and domestically and additional considerations.

While I believe in the benefits of the scanning technology and the importance of addressing radiation and nuclear threats to containers, this serves as another example of the pace of technology development differing from the rate of policy implementation. The lessons we are learning from this initial seven port deployment indicate a lot of promise for these technologies, but at the same time have allowed us to develop a more realistic vision of the challenges inherent in scanning the 11.6 million shipping containers that come to the United States from over 700 ports each year. As technologies mature, policies must be adapted to take full advantage of their benefits. Based on what we learn through these initial pilots, we will consider a full range of policy options that will allow the Department to best use the technologies to enhance security.

Securing Containers Through New Technology

The SAFE Port Act addresses the issue of container security standards and procedures. While DHS, as required by the Act, issued a letter on May 18, 2007 explaining that we will not be using the rule-making authority at this time, we strongly support and are continuing to seek opportunities to enhance supply chain security efforts, including enhancements to the security of the container. The potential use of Container Security Devices (CSDs) is a third area where the tension is evident between technology readiness and policy needs.

CSDs have the potential to increase the security of a container if they are able to accurately indicate whether a container has been opened by unauthorized personnel seeking to introduce dangerous and illicit materials or to remove the container's contents illegally.

However, when we discuss CSDs, we must recognize that there are also limits to the benefits: the financial and logistical costs of the devices and the significant infrastructure beyond the device itself that could be costly and challenging to deploy, as well as possible delays and other operational implications associated with response protocols.

We are developing a path forward that would explore the efficiency of these technologies and the degree to which they might enhance container security in very specific trade lanes. I look forward to sharing our strategy with this committee when it is finalized.

Partnerships and Collaborations

Before I discuss some of the specific provisions, I will offer a brief word on a second theme in the Department's overall approach to effectively implementing the SAFE Port Act: Partnerships and Collaborations. The Department's maritime and supply chain security doctrine is grounded on a commitment to deploy a strong, layered system. By deploying multiple, mutually-reinforcing security layers and tools, we diminish the risk associated with failure at a single point. To do this successfully, DHS must have equally strong partnerships with the trade and foreign governments who own and control most of the international supply chain.

The theme of partnership and collaboration, between DHS and other federal entities as well as between DHS, industry and the international community, is central to a number of programs and initiatives required by the Act. I would like to highlight some of the significant achievements within these partnership programs, touching upon international partnership such as the Container Security Initiative (CSI) and the Secure Freight Initiative (SFI), partnerships with domestic industry such as the Customs Trade Partnership Against Terrorism (C-TPAT), and the collaborative efforts between the Domestic Nuclear Detection Office (DNDO), other DHS offices, as well as other state, local, and federal entities.

Container Security Initiative (CSI)
The Container Security Initiative (CSI) and the Secure Freight Initiative (SFI) are true examples of successful bilateral and multilateral solutions to supply chain security. In both cases, DHS receives indispensable cooperation and support from foreign governments that has allowed us to establish a framework that will greatly aid our future efforts abroad.

Under CSI, we are partnering with foreign governments to identify and inspect high-risk cargo containers at foreign ports before they are shipped to our seaports and pose a threat to the United States and to global trade. We continue to make excellent progress in ports around the world. This fiscal year CSI expanded to 8 additional ports, and reached a milestone of 58 ports worldwide covering 85% of the container traffic destined to the United States.

Secure Freight Initiative (SFI)
As we continue to move forward on the next generation of CSI—the Secure Freight Initiative – I want to point out that this expands the CSI partnership to include, multiple foreign governments, the trade community, vendors of leading-edge technology, and vital U.S. government agencies, in particular the Department of Energy (DOE), who provides the Radiation Portal Monitors under their Megaports Program. I mentioned the Secure Freight Initiative previously, but I want to highlight here the fact that this initiative is the

culmination of healthy and vigorous cooperation at each of these levels: among U.S. Government agencies, between multiple foreign governments, and with the trade community and vendors of leading-edge technology.

Advance Security Filing Initiative ("10+2")
DHS fully appreciates the need to develop close partnerships with the private sector and industry as these groups own the assets and are responsible for the movement of goods throughout the global supply chain. Our efforts with the Advanced Security Filing Initiative as well as the Customs-Trade Partnership Against Terrorism (C-TPAT) program exemplify this collaborative approach.

As you know, the Safe Port Act required DHS to collect more detailed information on maritime cargo destined for importation into the United States. Working actively with the trade through trade advisory groups, such as the Departmental Advisory Committee on Commercial Operations (COAC) and through the trade community in general, DHS has developed the Advanced Security Filing (better known as the "10+2" data elements). The Advanced Security Filing will provide additional advanced cargo information that will enhance our ability to perform risk-based assessments prior to cargo being laden on a vessel overseas. A Notice of Proposed Rulemaking is currently under review but I want to assure you that DHS is committed to expediting this process to the extent possible.

Customs Trade Partnership Against Terrorism (C-TPAT)
CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) is an integral part of the DHS multi-layered strategy. CBP works with the trade community to ensure that our partners adopt stronger supply chain security measures across their international supply chains. Significantly, the program has enabled CBP to leverage supply chain security overseas where the U.S. government has no regulatory authority.

C-TPAT is an example of one of the successful programs supported by Congress through codification in the SAFE Port Act. The SAFE Port Act not only legislatively recognized C-TPAT, but also added greater accountability by mandating specific time frames for activities and greater program oversight. Again, I am pleased to report that DHS will meet all C-TPAT Safe Port Act requirements: CBP will validate all new partners within one year of certification, revalidate Tier 2 and Tier 3 members once every three years, and conduct yearly revalidations on some of the highest risk enrollment sectors such as the U.S./Mexico highway carriers.

Additionally, CBP has implemented a pilot program using third parties to validate supply chains where we currently lack full access. In May 2007, CBP selected 11 firms to act as validators in China because Chinese government continues to deny CBP personnel access to conduct supply chain security validations. I will note that interest in the pilot program has thus far been minimal. Of the more than three hundred (300) C-TPAT importers that were invited to participate in this voluntary pilot in June, less than a dozen importers have opted to do so to date. The primary concerns expressed by C-TPAT members involve sharing proprietary business and security data with a third party and the costs associated

with the validation, which, as outlined in the SAFE Port Act, must be incurred by the C-TPAT member.

Domestic Nuclear Detection Office (DNDO)
Since the authorization of the Domestic Nuclear Detection Office (DNDO) by the SAFE Port Act one year ago, DNDO has continued to strengthen its role within DHS. DNDO has successfully developed strong working relationships with CBP and USCG and is meeting the requirements outlined in the SAFE Port Act. Individuals from across the various government agencies have brought their knowledge and expertise to the table to help DHS create a robust program focused on the tools needed to detect and interdict nuclear or radiological material.

DNDO's comprehensive strategy for the deployment of radiological and nuclear detection equipment, submitted to Congress this year, provides an overview of some of DNDO's key activities, and I would like to touch on a few notable achievements.

Working closely with other DHS components, DNDO has made excellent progress in deploying radiation detection technology at our busiest ports resulting in the radiation scanning of just over 94 percent of all incoming seaborne cargo into the United States. By the end of this calendar year, 98 percent of all containerized sea cargo entering the United States at the 22 busiest ports will be scanned for radiological and nuclear threats.

Furthermore, DNDO is currently testing the next generation of radiation detection equipment, known as Advanced Spectroscopic Portals, at eight locations nationwide – at Piers A and J in Long Beach, at the APM and PNCT Terminals in Newark, at the Colombia and World Trade bridges in Laredo, at the Blue Water Bridge in Port Huron, and at the Fort Street crossing in Detroit. Future deployments of ASPs, pending Secretarial certification, will allow CBP to quickly differentiate between real threats and benign materials, such as kitty litter or granite.

The SAFE Port Act also required DNDO to establish an Intermodal Rail Radiation Detection Test Center. This was a forward-thinking requirement and one that DNDO strongly supports. The Port of Tacoma was selected as the location of the Rail Test Center because more than 70 percent of its total import cargo volume is handled by rail at multiple intermodal rail terminals. DNDO is working diligently with CBP and the Port of Tacoma to begin testing the operational needs, as well as evaluating innovative technical solutions, to fit the unique radiological and nuclear detection requirements of intermodal rail terminals.

DNDO also recently announced the West Coast Maritime pilot program, which is beginning in the Puget Sound region of Washington State and will expand into San Diego, California. The three-year pilot will provide maritime radiation detection capabilities for State and local authorities with the goal of reducing the risk of radiological and nuclear threats that could be illicitly transported on recreational or small commercial vessels. This effort is another example of the close coordination between DNDO and other DHS components including CBP and USGC.

Path Forward

Let me conclude with a few comments related to the Department's path forward. Our focus on risk management and security is driven by Congressional mandates and media interest but also by informed judgments about other areas of potential risks.

Over the last several years, the focus on threats from large commercial vessels and containerized cargo has been significant. As we continue to discuss the risks and threats to maritime container security, the department is also focusing on other threats to our ports, such as the kind demonstrated by the attack on the U.S.S. Cole or the French tanker, The Limburg. The USCG and CBP are working closely to expand our efforts to secure small maritime crafts. Although the overwhelming majority of small craft owners and operators are upstanding citizens and law-abiding mariners, various small vessels operate with great autonomy and anonymity in close proximity to critical maritime infrastructure and key resources, creating a potential for terrorist exploitation.

DHS believes that preventive, but reasonable, measures are necessary to address potential small vessel threats, ranging from smuggling Weapons of Mass Destruction (WMDs) across our borders, to their use as a water-borne improvised explosive device or as platforms for attacks against our nation's critical infrastructure. We are currently developing a National Strategy to address these risks by: (1) Implementing a layered approach; (2) leveraging a strong partnership with the small vessel community and public and private sectors to enhance maritime domain awareness; (3) leveraging technology to enhance our ability to detect, determine intent, and interdict small vessels when necessary; and (4) enhancing coordination, cooperation, and communication among various stakeholders, including Federal, state, local, tribal, and territorial agencies, as well as international partners.

The Department is working closely with other government departments and agencies, with industry, and the international community to establish workable solutions to improve supply chain security.

We recognize the importance of having a realistic schedule for technological development and the importance of establishing strong international and public-private partnerships. We applaud the ambitious goals established in the SAFE Port Act and continue to work energetically to implement them. I would like to thank the Senate Committee on Homeland Security and Governmental Affairs again for this opportunity to discuss our efforts within the context of the SAFE Port Act.

This completes my prepared statement. I would be happy to answer to any questions you may have.