SAFE PORT ACT

ONE YEAR LATER

October 2007

Source: Department of Defense

Prepared by the Republican Staff of the Committee on Homeland Security
Rep. Peter T. King (R-NY), Ranking Member

TABLE OF CONTENTS

SAFE Port Act: One Year Later
Executive Summary

On October 13, 2006, the President signed H.R. 4954, the Security and Accountability For Every (SAFE) Port Act, into law. The implementation of this bipartisan legislation, which passed both the House and Senate by overwhelming majorities, will enhance America's existing port and maritime security by expanding upon previous initiatives, and more importantly will develop new programs and allocate additional resources to address critical gaps in maritime and cargo security.

This Committee on Homeland Security Republican staff report examines the Department of Homeland Security's efforts to implement the 90-plus mandates within the SAFE Port Act, with particular focus in the following key areas:

Increased U.S. Port Security Readiness and Preparedness
The law established a timetable for the implementation of the Transportation Worker Identification Credential program, authorized the Port Security Training Program, and amended the Port Security Grant Program to include risk-based allocation.

Enhanced layered-security throughout International Supply Chain
The law codified the Customs-Trade Partnership Against Terrorism and the Container Security Initiative, required minimum standards for securing containers, authorized an integrated cargo scanning system pilot project, and mandated an enhanced high risk targeting system.

Leveraged Intelligence & Information Sharing:
The law established port security interagency operational centers at all high risk ports and enhanced awareness in the nation's maritime domain through long range vessel tracking.

At the direction of the Republican Members of the Committee on Homeland Security, the staff has conducted a year long review of implementation of the SAFE Port Act and reports back that the Department of Homeland Security has completed a majority of the requirements consistent with the intent of the law. But while the Committee applauds Department of Homeland Security for its dedication and determination, several important deadlines have been missed and much still needs to be done. Al Qaeda has demonstrated both its desire and ability to attack maritime transportation systems around the globe. Here in the United States, our more than 360 seaports are critical to both our economy and security. Our nation's seaports generate approximately 8.4 million American jobs, adding nearly $2 trillion to the U.S. economy annually, and facilitating critical defense logistics operations.[1] Therefore, it is critical that the United States continue to enhance its multi-layered, international defense to counter the increasing threat from those who wish to attack this key part of the American economy.

[1] "The Local and Regional Economic Impacts of the US Deepwater Port System," Martin Associates, September 5, 2007. http://aapa.files.cms-plus.com/PDFs/2006%20port%20impact%20report%20summary-JohnMartin.pdf.

For example, a container-based nuclear or radiological "dirty" bomb attack on a major U.S. port would tragically cost thousands of innocent lives and also result in the loss of billions of dollars. Experts' estimates vary from losses of $600 million per day[2] to $2 trillion a year[3] if a major U.S. port were struck by a 10- to 20-kiloton nuclear bomb.

The SAFE Port Act was crafted to strengthen our nation's maritime security in order to prevent this and other types of catastrophic attacks. The following report is a look at the key requirements of the SAFE Port Act and the implementation status:

SAFE Port Act Requirement	**Implementation Status**
Transportation Worker Identification Credential (TWIC) – a secure identification program that issues ID cards for individuals with access to secure areas of United States ports.	The Transportation Security Administration (TSA) published the TWIC Final Rule on January 1, 2007 *in accordance with the mandate.* TSA did **not meet deadlines** for deploying the TWIC at ten priority seaports by July 1, 2007. TSA did **not meet deadlines** for establishing five pilots to test TWIC readers at seaports by April 13, 2007. It is unlikely that TSA will meet the deadline of January 1, 2008 for distributing TWIC to workers at the top 50 ports.
Port Security Grant Program – allocating grants to seaports based on risk.	The Department of Homeland Security allocated grants based on risk *in accordance with the mandate.* The Coast Guard issued a report to Congress on the risk methodology for grants *in accordance with the mandate.*
Port Security Training & Exercises – a program for port security exercises	The Department of Homeland Security <u>is developing</u> a plan to restructure training and exercises programs to include recovery and involve all stakeholders.
Automated Targeting System – a program to target high risk containers coming to the United States.	Customs and Border Protection (CBP) <u>is developing</u> regulations to require additional advanced data from the private sector to use for high risk targeting.
Container Security Standards and Processes – a requirement to set minimum standards and procedures for securing	CBP did **not meet deadlines** for initiating regulations to establish minimum standards for securing containers by January 13, 2007.

[2] National Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California, Port Case Study, http://www.usc.edu/dept/create/research/case_studies.htm#ports.
[3] Haveman, Jon and Howard Shatz, eds., *Protecting the Nation's Seaports: Balancing Security and Cost*. (San Francisco: Public Policy Institute of California, 2006), 8.

maritime containers.	CBP did **not meet deadlines** for issuing an interim final rule by April 13, 2007. CBP submitted a letter explaining the delay in issuing the minimum standards on May 18, 2007 *in accordance with the mandate.*
Container Security Initiative – a program to place U.S. personnel in foreign seaports to target and inspect high risk containers.	CBP has notified the Congress in advance of announcing a new foreign ports participation in the Container Security Initiative *in accordance with the mandate.* CBP has coordinated with the Department of Energy's Megaports program to provide radiation detection equipment at foreign ports participating in the Container Security Initiative *in accordance with the mandate.* CBP did **not meet the deadline** for issuing a report to Congress on the Container Security Initiative by September 30, 2007.
Secure Freight Initiative – a program to test and evaluate the value and feasibility of conducting 100% scanning of maritime containers bound for the United States in 3 pilot locations overseas.	CBP designated 3 foreign seaports as pilot sites for 100% scanning before January 13, 2007 *in advance of the mandate.* The pilot sites became operational before October 13, 2007 *in advance of the mandate.* It is likely that CBP will provide a report to Congress on the pilots no later than April 13, 2008 *in accordance with the mandate.*
Customs-Trade Partnership Against Terrorism (C-TPAT)– a public-private partnership requiring additional security measures be implemented by the private sector in return for reduced and expedited container inspection.	CBP established minimum requirements for Customs-Trade Partnership Against Terrorism (C-TPAT) applicants and established a tiered structure for C-TPAT members *in accordance with the mandate.* CBP has developed a process to conduct on-site security checks of C-TPAT members within one year of joining the program and then to conduct a follow-up review within four years *in accordance with the mandate.* CBP submitted a report to Congress on a pilot program for utilizing third party entities to conduct C-TPAT *in accordance with the mandate.* However, the report was submitted late.
Long Range Identification and Tracking – a program to identify and track vessels	The current Coast Guard strategy to develop a long range vessel tracking system by April 2007 may not meet the intent of the law. Additional information is needed on

approaching the United States.	the Coast Guard's developing plan to enhance long range vessel tracking based on the October 3, 2007 Notice of Proposed Rulemaking .
Interagency Operations Centers for Port Security – a requirement to establish command centers at high risk ports.	The Coast Guard is developing a plan to establish interagency operational centers for port security at all high-priority ports no later than October 13, 2009.

To assist the Department of Homeland Security in implementing the mandates from the SAFE Port Act according to the Congressional intent, as well as address new challenges to securing the maritime transportation system in the future, the following recommendations are included in the report:

In general –

- ✓ Congress must maintain funding at the SAFE Port Act authorized levels for port security programs to ensure resources are available for implementation
- ✓ The Department of Homeland Security must provide all requested information and reports to Congress as mandated in the SAFE Port Act according to the specified deadlines

Protecting U.S. Ports –

- ✓ Test the Transportation Worker Identification Credential reader system prior to field deployment, train workers to respond to system malfunctions, and incorporate existing port access screening programs
- ✓ Continually communicate with key stakeholders to ensure a smooth rollout of the TWIC program, ensure enrollment centers are accessible, and establish an effective redress program for those wrongly flagged
- ✓ Continue to allocate port security grants on the basis of risk
- ✓ Include recovery and resumption of trade considerations in all port security training and exercise programs and involve all key stakeholders

Securing the International Supply Chain –

- ✓ Quickly issue the Notice of Proposed Rulemaking for the collection of additional advanced data, address private sector concerns, and consider the impact on small business
- ✓ Conduct random container searches to better inform and test high risk targeting capabilities
- ✓ Engage the international community and foreign governments participating in the Secure Freight Initiative to ensure 100 percent container scanning is feasible, enhances security and does not unduly interfere with the flow of commerce
- ✓ CBP must maintain the ability to conduct timely and quality validations
- ✓ CBP should consider additional benefits for top tier C-TPAT members

- ✓ CBP should develop mechanisms for sharing information on threats and vulnerabilities with C-TPAT members

Enhancing Intelligence & Information Sharing –

- ✓ The Coast Guard must continue to partner with the private sector and maritime exchanges to identify a better way to expand their awareness of vessels in the maritime domain
- ✓ The Coast Guard must develop policy and procedures for identifying, tracking

Overview:
Securing the Maritime Transportation System

One year ago, H.R. 4954, "the Security and Accountability For Every (SAFE) Port Act of 2006," was signed into law by President Bush after passing the House of Representatives by a vote of 421-2 and the Senate by a vote of 98-0. An overwhelmingly bipartisan effort, the SAFE Port Act bolstered America's existing maritime and port security framework by adding layers of defense through enhancing the security of United States domestic seaports; securing the global supply chain from point of origin to final destination; and facilitating intelligence and information sharing. The SAFE Port Act recognized the importance of a multi-layered, international defense in which transparency and awareness of possible threats are present throughout the international supply chain.[4] Moreover, the SAFE Port Act acknowledged the critical role of the private sector—those who own and operate the cargo, conveyances and facilities—in securing all parts of the Maritime Transportation System.

During the past year, the Department of Homeland Security (DHS) has made significant strides toward implementing the more than 90-plus mandates laid out in the SAFE Port Act. The Government Accountability Office (GAO) recently released its Department of Homeland Security "Progress Report on Implementation of Mission and Management Functions," which reported that DHS has achieved "substantial" progress in the maritime environment, the highest grade possible. Such a grade required general achievement of 75% of the 17 performance expectations in the area of maritime security. GAO recognized the efforts of DHS, particularly the U.S. Coast Guard and Customs and Border Protection (CBP), as well as other federal, state, and local agencies to enhance their security policies and strategies across the port and maritime domain. Their commitment to improve port readiness, preparedness and response; secure the international supply chain; bolster nuclear, chemical, biological, radiological, nuclear and explosive detection and deterrence capabilities; and improved intelligence and information sharing have strengthened our maritime security. Nevertheless, we must remember there are still gaps in our port and

[4] The SAFE Port Act, Table of Contents, Section 2 defines the International Supply Chain as the end-to-end process for shipping goods to or from the United States beginning at the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination.

maritime security systems, and radical terrorists remain committed to exploiting those security gaps and attacking American ports.

Maritime Terrorist Threats

Historically, terrorists have not focused on the maritime venue due to the low probability of media coverage out at sea, thus, losing the "spectacular" visual that affects the American consciousness.[5] However, modern terrorists have broadened their goals from a short-lived "spectacular" attack to include "dual purpose targets" with continuing economic damage.[6] Therefore, as we close gaps in our port and maritime security, America must remain vigilant as terrorist groups will continue to adapt their tactics and alter their targets to exploit security gaps wherever they can find them.

Al Qaeda has already demonstrated their desire and ability to use maritime transports and cargo containers to attack maritime targets. For example, al Qaeda's small boat suicide doctrine produced the deadly attacks on the *USS Cole* and MV Limburg in October 2000 and October 2002, respectively. The *USS Cole* was attacked in the harbor at Aden, Yemen by a small suicide boat laden with explosives, killing 17 U.S. Navy sailors and resulting in more than $250 million in damage to the ship.[7] The MV Limburg, also attacked by a small suicide boat packed with explosives, lost more than 20 percent of its crude oil cargo in the attack. The economic impact was also significant, with some experts estimating the attack on the MV Limburg cost the Port of Yemen "approximately $180 million over six months."[8] The significance of this attack was also highlighted in an al Qaeda communiqué issued shortly after the MV Limburg bombing:

> "If a boat which didn't cost $1,000 managed to devastate an oil tanker of that magnitude, imagine the extent of the danger that threatens the West's commercial lifeline, which is petroleum…The operation of attacking the French oil tanker is not merely an attack against a tanker--it is an attack against international oil transport lines and all its

[5] Lorenz, Akiva J. "Al Qaeda's Maritime Threat," April 15, 2007, http://www.ict.org.il/apage/11847.php
[6] Venzke, Ben N. and Aimee Ibrahim, "Al-Qaeda Threat to Oil Industry and U.S. Allies," Military Intelligence Professional Bulletin, Ft Huachuca: October-December 2003, Vol. 29, Issue 4.
[7] Nagle, David, Naval Sea Systems Command Public Affairs, U.S. Navy, "USS Cole Rejoins Fleet," April 2002, http://findarticles.com/p/articles/mi_pnav/is_200204/ai_2302032961
[8] Cordner, Lee and Dale Rentsch. "Terrorism and Maritime Trade: The Next 'Soft Target'?", What's Next, (December 2003), p. 3, quoted in J.A. Boutilier, "Reflections on the New Indo-Pacific Maritime and Naval Environment," *Journal of the Australian Naval Institute*, no. 114 (2004): 21-27.

various connotations."[9]

M/V Limburg, Following an al Qaeda attack near Yemen in October 2002
Photo courtesy of The Jamestown Foundation

Attacks on vessels are not the only method considered by terrorists in the maritime environment. After the capture of Khalid Shaikh Mohammed, al Qaeda's third in command and the mastermind behind the September 11th attacks, Mohammed admitted to offering to invest $200,000 in a Pakistani garment business in exchange for access to its shipping containers bound for Port Newark in the New York/New Jersey harbor complex.[10] While that plan was not executed, radical terrorist groups have at least twice demonstrated success in stowing operatives in cargo containers. The first occurred in October 2001 in the Italian port of Gioia Tauro, where a suspected al Qaeda operative was discovered in a container "furnished as a makeshift home with a bed, water, supplies…two mobile phones, a satellite phone, a laptop computer, and several cameras."[11]The second occurred in Port Ashdod, Israel, in March 2004, where two Palestinian terrorists hiding behind a secret compartment in a container emerged in a post-container screening area and killed 10 port workers.[12]

[9] Libicki, Martin C. "Exploring Terrorist Targeting Preferences," The RAND Corporation, 2007, p. 40. http://www.rand.org/pubs/monographs/2007/RAND_MG483.pdf.
[10] Richardson, Michael. "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction," Institute of South East Asian Studies, Singapore, February 25, 2004.
[11] Ibid.
[12] Howland, Jonathan. "U.S. Starting to Focus on Maritime/Seaborne Terror Assault on Israeli Ashdod Port Kills 10, Mega Attack Narrowly Avoided," Jewish Institute of National Security Affairs, April 16, 2004,

Al Qaeda sees the maritime venue as a target rich environment because the challenges of securing port infrastructure from both sea and land are immense, while a relatively small financial investment by al Qaeda can yield a large return.[13] Al Qaeda can utilize the ship, the crewmembers and the cargo, either collectively or separately, to carry out a maritime attack.[14] Following the capture and interrogation of Abdul al-Rahim al-Nashiri, the United States learned of al Qaeda's wide ranging maritime targets throughout the West, including military vessels in the Straits of Gibraltar and Hormuz, oil tankers in the Persian Gulf and beyond, even cruise ships and passenger ferries. The methods of attack also varied, ranging from divers with underwater explosives to speed boats laden with explosives, or simply packing a departing ship with explosives.[15]

U.S. Ports: Gateway for Domestic and International Commerce

DHS has the difficult job of protecting America's maritime transportation infrastructure, while at the same time facilitating the free flow of commerce—two missions that can often be contradictory. America's more than 360 ports are the lifeblood of the global economy, serving as the gateway for more than $3.6 billion worth of American imports and exports.[16] According to an August 2007 Martin Associates port-sector economic impact study, United States deep-draft seaports and seaport-related businesses generated approximately 8.4 million American jobs and added nearly $2 trillion to the economy.[17] Others estimate that approximately "one-third of the U.S. economy depends on the people, goods, and services that traverse the world's oceans."[18]

---

http://www.jinsa.org/articles/articles.html/function/view/categoryid/1701/documentid/2454/history/3,2360,655,1701,2454.

[13] "Bin Laden: Goal is to bankrupt U.S.," CNN.com, November 1, 2004, http://www.cnn.com/2004/WORLD/meast/11/01/binladen.tape/index.html

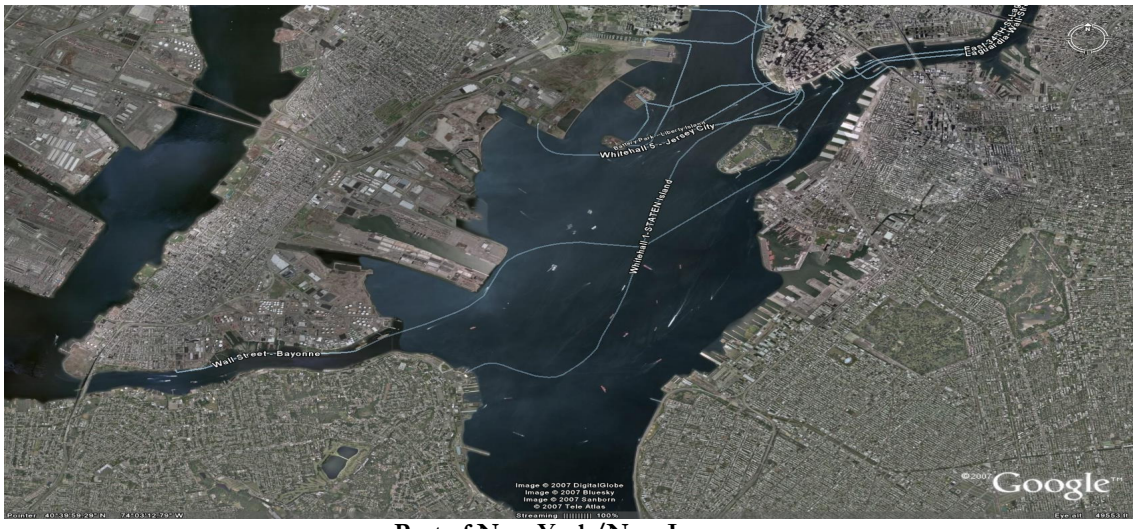
[14] Boutilier, J. A. "Reflections on the New Indo-Pacific Maritime and Naval Environment," *Journal Of the Australian Naval Institute*, no. 114, (2004): 21-27.

[15] Lorenz, Akiva J. "Al Qaeda's Maritime Threat."

[16] Nanto, Dick K. "U.S. International Trade: Trends and Forecasts," Congressional Research Service, Updated July 17, 2007.

[17] "The Local and Regional Economic Impacts of the US Deepwater Port System," Martin Associates, September 5, 2007. http://aapa.files.cms-plus.com/PDFs/2006%20port%20impact%20report%20summary-JohnMartin.pdf.

[18] Carafano, James J., Ph.D. and Martin E. Andersen, "Trade Security at Sea: Setting National Priorities for Safeguarding America's Economic Lifeline," The Heritage Foundation, Backgrounder No. 1930, April 27, 2006.



Port of New York/New Jersey

These estimates clearly highlight the importance of SAFE Port Act mandated initiatives. It is absolutely critical that DHS speed up the implementation of lagging programs that leave the maritime system vulnerable to terrorist attacks, while continuing to enhance and strengthen existing security programs. While estimates vary, there is no doubt that a container-based nuclear attack on a major U.S. port could cost hundreds of thousands of lives and prove devastating to our economy.

In order to better understand the potential economic consequences, consider the following expert's estimates:

- A June 2006 Public Policy Institute of California report entitled "Protecting the Nation's Seaports: Balancing Security and Cost" estimates a Los Angeles -Long Beach port closure of one year due to a radiological attack could reach upwards of $45 billion in "national economic damage, including direct costs, indirect costs, and induced costs."[19]

- An August 2006 RAND report entitled "Considering the Effects of a Catastrophic Terrorist Attack" modestly estimated that the detonation of a 10-kiloton nuclear

[19] Haveman, Jon and Howard Shatz, eds., *Protecting the Nation's Seaports: Balancing Security and Cost*. (San Francisco: Public Policy Institute of California, 2006): 8.

bomb in a shipping container on the pier of the Port of Long Beach would cost up to $1 trillion.[20]

- An Abt Associates study prepared for the U.S. Department of Transportation estimated that a 10- to 20-kiloton nuclear detonation at a major seaport would kill fifty thousand to one million people and result in property damage and trade disruption of $150 billion to $700 billion, with indirect costs adding up to more than $1.4 trillion. Their total one-year economic cost to the U.S. could amount to $2 trillion.[21]

[20] Meade, Charles and Roger C. Molander. "Considering the Effects of a Catastrophic Terrorist Attack," August 2006, The RAND Corporation, xvi.
[21] Abt, Clark C. "The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability," Abt Associates, Inc., April 30, 2003.

Examining the SAFE Port Act

Republican Staff of the Committee on Homeland Security conducted a thorough review of the 90-plus mandates in the law and have presented the following updates to the Republican Members responsible for maritime and cargo security oversight. The report examines the status of security measures of U.S. ports, the international supply chain, and intelligence and information sharing. The report does not include information on every area mandated by the SAFE Port Act but rather focuses on the major requirements in each of those three areas and offers recommendations for further improvement.

Protecting U.S. Ports

Title I of the SAFE Port Act addresses security of U.S. domestic seaports. The focus is on ensuring that only authorized individuals who have passed background checks are able to access secure areas of seaports, that high-risk ports receive federal grants to enhance security, and that training and exercises are conducted on regular basis and involve all port stakeholders.

Transportation Worker Identification Credential

"The greatest threat vulnerability to maritime infrastructure may be internal threats, i.e., employees who have an intimate knowledge of operations and facilities and access to transportation and port assets."[22]

-Maritime Security Working Group

There are over 2,800 ports around the globe where hundreds of thousands of port workers facilitate the flow of more than 230 million containers and other cargo that move through the world's ports annually.[23] Maritime commerce analysts estimate that about 90% of the world's trade, worth over $1 trillion, is carried by sea on more than 50,000 ships by more than 1.25 million seafarers. Prior to September 11th there was no widely enforced security system throughout the maritime transportation system. In fact, maritime transportation workers were permitted to move about freely during U.S. port calls and cargo security was essentially non-existent.[24]

---

[22] Carafano, James J. and Alane Kochems. "Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism," The Heritage Foundation, February 17, 2005, p. 16.
[23] Richardson, Michael. "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction."
[24] Ibid.

Given the enormous dependence of the U.S. and global economy on the maritime shipping industry, it was obvious something needed to be done to reduce the number of unauthorized individuals accessing seaports. Thus Congress passed bipartisan legislation in both the Maritime Transportation Security Act (MTSA) of 2002 and SAFE Port Act of 2006 to require a secure access system for our nation's ports.

The Transportation Worker Identification Credential (TWIC) program is designed to secure restricted areas of vessels and port facilities by issuing transportation workers a secure identification card including biometrics, such as fingerprints and digital photographs. The card, which is only issued after the worker has passed both a biometric and biographic background check, allows the worker unescorted access at ports. The TSA initially began research and development for a transportation identification card system prior to the passage of MTSA in 2002, yet, in the four years between MTSA and SAFE Port, TSA failed to deliver an effective system. Congress, frustrated after four years without a final product, mandated a risk-based implementation schedule for TWIC in the SAFE Port Act to quickly close gaps in our transportation security. The chart below details the requirements, deadlines and status of TWIC as of October 4, 2007.

SAFE Port Requirement	**Deadline**	**Status**
DHS must publicize final regulations for issuing TWIC cards	January 1, 2007	DHS published TWIC Final Rule on their website on January 1, 2007
TWIC card reader pilot must be deployed at five distinct geographic sites to include vessels and facilities	April 2007	DHS issued the TWIC card reader specifications.[25] The card pilot program is <u>delayed</u> pending further TWIC card rollout.
1st progress report due to Congress on implementation of TWIC (a bi-annual requirement)	April 2007	No formal report was provided; however, testimony was received before Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism on April 26, 2007.
TWIC cards must be issued at top 10 priority ports	July 1, 2007	<u>Failed to meet deadline</u> due to extended testing of technology. DHS

[25] Federal Register, September 21, 2007, Vol. 72, No. 182, Pg. 53784

		is rolling out in Wilmington, Delaware on October 16th, followed by an additional eleven ports by mid-November.
2nd progress report due to Congress on implementation of TWIC	October 2007	No formal report has been received; however, testimony is scheduled before the Committee on Homeland Security on October 31, 2007.
TWIC cards must be issued at remaining top 50 priority ports	January 1, 2008	Unclear whether DHS will meet this deadline, although it is unlikely that all workers at the top 50 ports will have received their cards by the deadline.

Although TSA missed the SAFE Port deadline to implement TWIC at the top ten priority ports by July 1, 2007, DHS has now rolled out the program at the first location in Wilmington, Delaware, and will expand to 11 more ports by mid November. DHS has also announced its quarterly roll out schedule for fiscal year 2008.

While the current issues that have plagued the TWIC program are disappointing, it is important that the rollout of TWIC not only strengthen our nation's security but is also convenient and user friendly to the more than 750,000 transportation workers affected by it. To this end, we recommend TSA, in consultation with the Coast Guard, consider the following:

- ✓ Thoroughly test TWIC card reader systems prior to deploying them into the field
- ✓ Maintain continuous collaboration and communication with key stakeholders – ports, industry and labor unions – to ensure smooth rollout and sustained security effectiveness
- ✓ Incorporate and recognize existing screening programs, reducing burdensome costs and delays created by multiple programs performing the same function
- ✓ Establish an effective redress program for those wrongly flagged by TWIC, including a waiver and appeals process that fairly and quickly decides workers claims
- ✓ Develop, share, and train workers on policies and procedures to handle port or system-wide breakdowns in the reader verification system

- ✓ Ensure enrollment centers are accessible and convenient to the 750,000 transportation workers required to enroll

Port Security Grant Program

"Simply put, our goal is to put our resources where the risk is the greatest, and where the funds will have the most impact."[26]

-DHS Secretary Michael Chertoff
January 9, 2007

Since the inception of the Port Security Grant Program (PSGP) in 2002, DHS has given $1,078,445,267 dollars to U.S. ports to enhance security and readiness.[27] Initially, the grants were awarded to over 125 large, medium and small U.S. port areas[28] since the MTSA of 2002 required "fair and equitable"[29] distribution. However, during the third round of PSGP grants in 2005, DHS relied more on the risk to a port to bring the list of eligible U.S. ports down to 66.[30] In fiscal year 2006, DHS again changed grant eligibility based on the U.S. Coast Guard's Port Criticality List, which used factors such as cargo and passenger volume, presence of critical infrastructure/key assets, and strategic importance to identify the 100 most critical ports essential to the viability of the U.S. maritime transportation system.[31] The SAFE Port Act amended the MTSA provision to make the risk-based funding system more permanent, grouping the most critical ports into four different tiers, with Tier 1 representing the highest risk ports and Tier 4 representing the lowest risk.[32] The Coast Guard met the SAFE Port Act deadline to submit a report to Congress describing the risk-based methodology used to distribute port security grant funds on the basis of risk.

---

[26] Remarks by Secretary Michael Chertoff at a Press Conference on the Fiscal Year 2007 Infrastructure Protection Grants Program, January 9, 2007, http://www.dhs.gov/xnews/releases/pr_1168438375963.shtm
[27] U.S. Department of Homeland Security, Office of Legislative and Governmental Affairs email to Republican Staff, September 18, 2007.
[28] U.S. Department of Homeland Security, Office of Inspector General. *Review of the Port Security Grant Program*. OIG-05-10, January 2005, p. 30.
[29] 46 U.S.C. 70107(a).
[30] U.S. Department of Homeland Security, Office of Domestic Preparedness. *Fiscal Year 2005 Port Security Grant Program*. 2005, p. 4.
[31] U.S. Coast Guard, Infrastructure Protection Program (IPP), FY 2006 Port Security Grant Program (PSGP) Fact Sheet Series: PSGP Overview, http://www.uscg.mil/d8/sector/UMR/FY%202006%20PSGP%20Fact%20Sheet%20FINAL.pdf
[32] U.S. Department of Homeland Security, Press Office, "DHS Awards $399 Million in Grants to Secure the Nation's Critical Infrastructure, September 25, 2006.

TIER 1 PORTS	FY07 FUNDING[33]
New York-New Jersey	$42,168,171
Puget Sound (Seattle, Tacoma, Everett, Anacortes)	$24,033,412
Houston-Galveston	$23,726,722
Los Angeles-Long Beach	$23,456,550
New Orleans (Baton Rouge, New Orleans, Plaquemines, and South Louisiana)	$22,256,672
Bay Area (Oakland, Richmond, San Francisco and Stockton)	$20,353,200
Sabine-Neches River (Beaumont, Port Arthur, TX)	$11,263,459

DHS has met the SAFE Port Act deadline requiring a report detailing the risk-based methodology of the port security grant program. This shift enables DHS to allocate grant funds where it is needed most. Additionally, we recognize the need for Congressional support to maintain funding at the authorized level of $400 million annually to ensure that our ports have the federal support necessary to implement many of the security enhancements.

Port Security Training & Exercises

"PortSTEP is designed to benefit maritime and surface transportation security communities throughout the U.S. via a suite of training exercises, evaluations and accompanying information technology products. This information will prove invaluable as we work to balance freedom of commerce and protection of our nation's transportation system."[34]

-Noreen Brown
TSA's PortSTEP Project Officer

Training and exercise programs in U.S. seaports play a critical role America's maritime transportation security. The Port Security Training and Exercise Program (PortSTEP), under the direction of the TSA and the U.S. Coast Guard, bridges four Homeland Security Presidential Directives and serves as a strategic outreach, training, and education tool for the Coast Guard's Area Maritime Security Committees. PortSTEP

[33] U.S. Department of Homeland Security, Overview: Fiscal Year 2007 Infrastructure Protection Program Final Awards, May 10, 2007, p. 15-16; and Fiscal Year 2007 Supplemental, Infrastructure Protection Program: Port Security Grant Program, Program Application and Guidance, August 16, 2007, p. 3.
[34] U.S. Coast Guard, Fifth District Public Affairs Office, "Port of Philadelphia Conducts Maritime Security Exercise," August 21, 2007, http://www.piersystem.com/go/doc/651/169563/

initially received $20 million in 2002's Supplemental Appropriations Act to fund more than 40 exercises through October 2007.[35]

Source: U.S. Coast Guard

The SAFE Port Act enhanced the port security exercise program mandated by the Maritime Transportation Security Act of 2002, requiring DHS to consolidate all of the existing port security exercise programs. Congress also instructed DHS to establish a program designed to regularly conduct port-specific exercises followed by after action discussions of lessons learned among all participants. Additionally, the port exercise program must include preparedness, prevention, response, and recovery.

TSA reports that PortSTEP has increased information sharing among all key maritime and surface transportation stakeholders, enhanced coordination, expanded membership in the Coast Guard's Area Maritime Security Committees, and demonstrably strengthened our maritime transportation system's security.[36] Following the final PortSTEP exercise scheduled for October 2007, TSA and the Coast Guard will transition PortSTEP to the newly formed Intermodal Security Training and Exercise Program (I-STEP), enabling the program to broaden the scope of the exercises to include recovery and resumption of

[35] Transportation Security Administration, Office of Legislative and Governmental Affairs, PortSTEP briefing before Committee on Homeland Security Staff, September 17, 2007.
[36] Ibid.

trade. While much has been done in implementing PortSTEP, the next challenge is for DHS to develop I-STEP and accomplish the following:

- ✓ DHS must provide the Committee a detailed schedule of I-STEP exercises to ensure adequate integration of recovery and resumption of trade.
- ✓ DHS must ensure participation among all key stakeholders, including labor representatives and the private sector.
- ✓ Failure to authorize and fund I-STEP could result in increased vulnerability of our transportation system, reduced coordination between federal, state, and local strategies, and reduced readiness, response, and recovery capabilities.

Securing the International Supply Chain

The maritime transportation system is critical to the international economy. Globally, 90 percent of cargo and half of the world's trade by value is transported by containers.[37] In 2006, nearly 12 million containers arrived at U.S. seaports, equaling about 32,000 containers per day.[38] Prior to September 11th, less than one percent of containers worldwide were screened.[39] However, following the September 11th terrorist attacks, securing maritime containers quickly became a Presidential and Congressional priority. The most common container scenario involved the detonation of a nuclear weapon or radiological "dirty" bomb in a major U.S. port. While there is much debate regarding al Qaeda's current desire and capability to conduct a container-based attack, there is absolutely no mistaking the potential for loss of life and the devastating effect on our economy.

The SAFE Port Act recognized the importance of extending security beyond our shoreline and our ports and increasing the opportunities to detect high risk maritime cargo through a layered defense that uses international and private sector partnerships. The SAFE Port Act requires additional advanced data for targeting high risk containers, calls for standards for securing containers en route to the U.S., and authorizes and enhances existing

[37] Ibid.
[38] Satement of Stewart Baker, Assistant Secretary, Policy, Department of Homeland Security, before the Senate Committee on Homeland Security and Governmental Affairs, "One Year Later: A Progress Report on the SAFE Port Act," October 16, 2007.
[39] Richardson, "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction."

security programs including the Container Security Initiative and the Customs-Trade Partnership Against Terrorism. Additionally, the SAFE Port Act recognized the importance of examining and evaluating the operational impact of 100 percent scanning through pilot programs rather than placing a hard mandate without regard for the logistical and economic viability.

Automated Targeting System

"We…believe in risk management – not risk elimination. If we tried to eliminate literally every risk, we'd fail, for the simple reason that risk elimination is impossible…Risk management lets us identify what should concern us most in terms of threats, map those threats against existing vulnerabilities, and take steps to mitigate the potential consequences."[40]

-DHS Secretary Michael Chertoff

DHS was created to specifically address a critical mission: prevent terrorists and terrorist weapons from entering the United States. The number of targets and avenues for terrorists to bring weapons into the Untied States are innumerable and the maritime environment, with millions of container movements in and out of the U.S., is a major challenge. It is essential that the Department maintain a robust targeting capability to select high risk containers for further examination without crippling the supply chain and hurting the global economy.

In the maritime cargo domain, CBP has utilized its authority to collect manifest data from carriers 24 hours before loading U.S. bound containers in foreign ports. This authority is often referred to as the "24-Hour Rule." CBP's Automated Targeting System (ATS) analyzes the data and generates a risk score for each container, enabling CBP targeters to identify high risk cargo that may require further examination. Congress, concerned that manifest data alone is not sufficient for a thorough targeting system, included language in the SAFE Port Act directing CBP to determine additional advanced data necessary for enhancing ATS and ensuring that all high risk containers are selected for additional inspection.

[40] Chertoff, Michael, Remarks at the University of Southern California DHS Center of Excellence on Security in the 21st Century, July 20, 2007, http://www.dhs.gov/xnews/speeches/sp_1184959845456.shtm

Source: U.S. Customs and Border Protection

In response to the SAFE Port Act, CBP announced in December 2006 an expansion of the 24-Hour Rule, requiring importers to provide specific pieces of commercial data and ocean carriers to supply additional information on containers. This proposal is known as "10+2" and would require the following pieces of additional advanced information for ATS:

Importer Trade Data Elements[41]	Explanation of Trade Data Elements
Manufacturer Name and Address	Information of entity that last manufacturers, produces, or grows the imported commodity
Seller Name and Address	Information on the last named overseas (foreign) seller on the transaction invoice/purchase order
Container Stuffing Location	Physical foreign location, street, city, country, where the goods were stuffed into the container prior to closing the container
Consolidator Name and Address	Foreign entity that physically stuffs the container prior to receipt by carrier for shipment to U.S. The address identifies the physical location of where the cargo is stuffed.
Buyer Name and Address	Last named buyer and address 24 hours prior to foreign lading
Ship to Name and Address	Named party/address on the transaction that will physically receive the merchandise

[41] U.S. Customs and Border Protection, CBP Proposal for Advance Trade Data Elements, Annex A: Proposed Data Definitions. http://www.cbp.gov/linkhandler/cgov/import/carriers/adv_data_elements.ctt/adv_data_elements.doc

Importer of record number	Unique identifying number of entity primarily responsible for the payment of duties or an authorized agent acting on that entity's behalf
Consignee Number	Unique identifying number of the entity to which the goods are to be consigned
Country of origin of the goods	Country in which goods are wholly obtained or produced, as defined in CFR 19 102.11, Subpart B – Rules of Origin
Commodity Harmonized Tariff Schedule number (6-digit)	Indicated initial classification required of a shipment prior to entry being filed. Provides specific identification of the commodity being ordered from the purchase order.
Carrier Trade Data Elements	**Explanation of Trade Data Elements**
Vessel Stow Plan	Consists of nine data elements concerning the vessel, the container, its contents and location on the vessel and load/discharge ports
Container Status Messages	Consists of five data elements detailing every action taken on a container during transport

According to CBP, this additional data will enhance their ability to assess risk, as well as make critical decisions during and immediately after an elevated threat alert or threat level.[42] As of October 2007, CBP had concluded the internal review of the regulations and submitted the proposal to the Office of Management and Budget for final approval.

There is significant concern within the private sector over how 10+2 implementation will affect business processes and the flow of commerce. For example, many wonder how many and which requirements on the list will measurably strengthen the targeting system, who should ultimately be required to report the data to CBP, and whether there is existing technology to integrate the new "10+2" data with the current requirements of the 24-Hour Rule.

Recognizing the need for a robust targeting system as well as the legitimate concerns of the private sector, the following recommendations are provided:

- ✓ CBP and the Commercial Operations Advisory Committee must consider the challenges "10+2" will impose on smaller importers in the U.S.

[42] Ibid.

- ✓ DHS should move quickly to issue the Notice of Proposed Rulemaking to allow the trade community to provide feedback.

- ✓ CBP should further clarify the security benefits of the requested data and ensure that the most appropriate party is assigned the responsibility for providing the data.

- ✓ CBP should continuously review the various cargo security programs' lessons learned and seek to apply them where applicable.

- ✓ CBP should continue to conduct random container searches to better inform and test ATS.

Container Security Standards and Processes

"We are developing a path forward that would explore the efficiency of these technologies and the degree to which they might enhance containers security in very specific trade lanes."[43]

-DHS Assistant Secretary Stewart Baker

The ability to secure containers en route and determine if they have been compromised is vital to securing the supply chain. Congress recognized that a myriad of technical and logistical challenges are facing the operational deployment of a next-generation container security device but was concerned that no standard existed for minimum security procedures for containers entering the United States.

The SAFE Port Act required the Secretary of Homeland Security to publicize a rule to establish minimum standards and procedures for securing containers in transit to the United States by April 13, 2007. This deadline was not met; instead, DHS issued a letter on May 18, 2007, stating they would not use the rule-making authority until DHS can "explore the efficiency of these technologies and the degree to which they might enhance container security."[44] The Congressional intent of the provision was that CBP would set minimum standards that would be updated as technology matures. The SAFE Port Act was amended by H.R. 1 (P.L. 110-53) on August 3, 2007, removing the SAFE Port Act enforcement deadline for minimum standards by 2009 and replacing it with an extension to issue the regulations by April 1, 2008. If the deadline is not met, H.R. 1 requires, as of October 15,

[43] Satement of Stewart Baker, Assistant Secretary, Policy, Department of Homeland Security, before the Senate Committee on Homeland Security and Governmental Affairs, "One Year Later: A Progress Report on the SAFE Port Act," October 16, 2007.
[44] Ibid.

2008, all containers entering the United States must use a high-security bolt seal that meets international standards.

Department of Homeland Security officials continue to assert that container security technology has not yet caught up with policy requirements, but they are working with the DHS Science and Technology Directorate to "determine the technical and administrative requirements for the [container security device]"[45] The Directorate is exploring various solutions to enhance DHS' cargo security programs. SAFECON, a crane mounted sensor system that detects and identifies dangerous cargo during normal ship load/unload operations, is a notable project currently under development. In addition, the Directorate is working on advanced container security devices, which will monitor the container's six sides for intrusion; Hybrid Composite Containers that utilize embedded security sensor technology within the container walls; devices that monitor container doors; Secure Cartons that monitor tampering of box, carton or pallet cargo; and a Marine Asset Tag Tracking System that provides remote communications capabilities for those security devices to transmit status information and alarms.[46]

Recognizing the importance of securing containers in the international supply chain without disturbing the legitimate flow of goods across the border:

- ✓ The Department of Homeland Security must move forward to establish a minimum standard for securing containers and develop processes to ensure that any compromised container is identified and reviewed.
- ✓ The Department of Homeland Security must work with the private sector and the international community to develop container security standards and evaluate new technology.
- ✓ Congress should continue to fund Science and Technology research and development programs focused on next-generation container security solutions that are effective and feasible for use in the supply chain.

[45] Remarks by R. Ralph Basham, Commissioner, Customs and Border Protection, on Container Security at the Center for Strategic and International Studies, July 11, 2007.
[46] Ibid.

Source: U.S. Customs and Border Protection

Container Security Initiative

"We are committed to using high-tech equipment and a smarter, more secure container to safeguard the supply chain, but realize that cooperation from our friends around the globe is our most potent weapon."[47]

-Commissioner W. Ralph Basham
U.S. Customs and Border Protection

Security experts and conventional wisdom argue that additional security measures overseas will better protect the U.S. from threats; our nation's borders should be the last line of defense. CBP has several initiatives to layer security throughout the supply chain and increase security at foreign ports of departure.

The Container Security Initiative (CSI) developed after September 11th places CBP Officers at foreign ports where there is high volume of U.S.-bound containers. U.S. personnel work with host nation Customs to target containers using the Automated Targeting System and inspect those containers deemed to be high risk before they are loaded onto the vessel. Currently, CSI is operational in 58 ports across Latin America, the

[47] "U.S. Customs and Border Protection Achieves Container Security Initiative Milestone with 58 Operational Ports." News Release; CBP Newsroom, September 28, 2007.

Caribbean, Europe, Africa, the Middle East and Asia. These ports account for 90% of all transatlantic and transpacific cargo imported into the United States.[48]

The SAFE Port Act recognized CSI as a cornerstone of the United States' multi-layered defense, authorizing $196 million each year between fiscal years 2007-2012. While Congress has not fully funded the program at the authorized level, modest increases have allowed CBP to expand the initiative[49] Additionally, the SAFE Port Act required CBP to develop minimum standards for technology and equipment used in CSI ports and mandated that a "do not load" order be issued for any container determined to be high risk but not inspected by the host government. A report was due to the Congress by September 30, 2007, on the effectiveness of CSI and a progress report in meeting the Congressional mandates. DHS has not yet submitted this report.

Secure Freight Initiative

"No one measure, procedure, or technology will provide a very high (90%-plus) probability of spotting a WMD carefully concealed in one of the 10 million containers arriving in the Untied States; 100 percent is a pure fantasy."[50]

-Stephen S. Cohen
Director, Berkeley Roundtable on International Economy

Building on the framework of the Container Security Initiative, Congress developed a mandatory pilot program to test and evaluate the concept of scanning up to 100 percent of U.S.-bound containers overseas. The SAFE Port Act required three overseas pilot sites to be selected by April 13, 2007, and for the pilots to become operational, scanning 100 percent of U.S.-bound containers for nuclear material through radiation and imaging scans, by October 13, 2007. All of the data would be transmitted back to the CBP National Targeting Center in Virginia for evaluation. DHS has met these SAFE Port Act mandates.

The Secure Freight Initiative (SFI), as this pilot has been labeled, is currently operational at three ports – Puerto Cortes, Honduras; Port Qasim, Pakistan; and

[48] U.S. Customs and Border Protection, "CSI In-Brief," October 3, 2007, http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml
[49] In fiscal year 2007, CSI received $139 million in H.R. 5441, the Department of Homeland Security Appropriations Act, 2007, while the House authorized $159 million in H.R. 1684, the Department of Homeland Security Authorization, 2008.
[50] Cohen, Stephen S. "Boom Boxes: Containers and Terrorism," *Protecting the Nation's Seaports: Balancing Security and Cost.* (San Francisco: Public Policy Institute of California, 2006): 107.

Southampton, United Kingdom. The Department decided to expand the mandate and conduct pilots at three additional locations in Oman, South Korea and Singapore; these sites are scheduled to be operational in the near future according to Department officials. A report on SFI is due to Congress on April 13, 2008. The report is to include the lessons learned from the pilot, an analysis of how the data is used in the targeting system, an evaluation of the effectiveness of the system in detecting nuclear material, an evaluation of the software and technology used to automatically identify anomalies, and an analysis of the feasibility of expanding the pilots. The information in this report is critical to determining the value and feasibility of the 100 percent scanning concept.

Source: U.S. Customs and Border Protection

While the SAFE Port Act mandate was designed to enable DHS to evaluate the results of the SFI pilot prior to enacting a permanent program, the Democrat-led 110th Congress has since mandated in H.R. 1 (P.L. 110-53) that 100% of all U.S . bound cargo be screened, an action done without considering the results of the SFI pilot. The decision to ignore results of the pilot program sparked outrage from U.S. allied governments and key maritime transportation stakeholders.

SFI participant nations such as Singapore volunteered to participate in the SAFE Port SFI pilot program because the program was designed to evaluate feasibility instead of mandating untested regulations. In an August 2007 letter to the Chairman of the U.S. House of Representatives Committee on Homeland Security, Singapore, home to the largest container port in the world, expressed deep concern about the "significant negative impact of 100% container scanning." The letter highlighted numerous technical concerns of the 100% scanning mandate, specifically, that "existing scanning technology does not support the fast and efficient scanning of containers, its cost is prohibitive, and the [Democrats'] bill does not address the issue of funding for 100% scanning."[51]

In addition, eight leading industry organizations, such as the World Shipping Organization and U.S. Chamber of Commerce, highlighted their concerns about the 100% scanning requirement in a letter to the Chairman and Ranking Member of the U.S. Senate Committee on Homeland Security and Governmental Affairs. They expressed concern that the Democrats' bill ignores the complexity of international relations, does not include a plan for funding the program, and that the bill lacks certain specifics. For example, will 100% scanning affect all 600 foreign ports that ship containers to the U.S. or just the 80 major ports which account for 95 percent of U.S. bound container traffic? Will the bill cause our major trading partners, including commercial, military and government cargoes, to enforce the same scanning requirements on the United States?[52]

In June 2006, the Washington Post editorial writers weighed in on the subject, expressing their concerns over 100% screening:

> "Before the "inspect every container" mantra becomes a national war cry, it's important to point out that this is a terrible idea. Someday, perhaps, advanced X-ray technology may be developed to the point where it's possible to beam a scanner at each one of the 11 million U.S.-bound containers at every port in the world and obtain an instant assessment of what's inside. But while some promising technologies are available, now is perfect, and all of them require a human being to analyze the scans. This not only takes time

[51] Republic of Singapore, Minister of Transportation, Mr. Raymond Lim, Letter to Chairman, U.S. House of Representatives Committee on Homeland Security, August 6, 2007

[52] Eight Party Letter to Senators Lieberman and Collins, U.S. Senate Committee on Homeland Security and Governmental Affairs, June 26, 2007

but also presumes the existence of thousands of trained scan readers around the world."[53]

DHS implemented the required SFI pilots in accordance with the SAFE Port deadline but in order to develop the program to its fullest potential;

- ✓ DHS must continue to engage host nation governments and key private stakeholders to ensure container cargo initiatives measurably increase security and do not unduly interfere with the flow of commerce.
- ✓ DHS should continue to support critical research and development at its academic centers of excellence.
- ✓ Congress must continue oversight as DHS moves to implement 100% scanning as it will ultimately impact U.S. businesses and consumers, as well as key foreign relations.

Customs-Trade Partnership Against Terrorism

"The International Cargo Security Council fully supports and encourages our members' participation in C-TPAT…C-TPAT gives us an opportunity to join in the war against terrorism…our companies and our families are the beneficiaries of this important program."[54]

-Scott Smith
Former Chairman, International Cargo Security Council

The Customs-Trade Partnership Against Terrorism (C-TPAT) is an unprecedented voluntary partnership between the public and private sectors that seeks to enhance security throughout the supply chain from the point of origin to delivery. This program was developed prior to the creation of the Department of Homeland Security and has been continued and expanded under the direction of CBP. As the lead agency, CBP works with the private sector to develop security measures to secure goods moving through the global supply chain from the manufacturer to America's shelves.

Initiated in November 2001 with just seven members, C-TPAT has grown to more than 7,400[55] certified members, who are divided into three separate tiers based on the status of the certification and validation of their security plans. Companies who more aggressively

[53] "The Right Kind of Security." *Washington Post* 01 June 2006: A-18.
[54] "ICSC's Innovative Solutions for C-TPAT." International Cargo Security Council, http://www.cargosecurity.com/ncsc/education-CTPAT.asp#eight%20reasons.
[55] DHS Staff briefing October 5th.

pursue their own security measures are rewarded, as an incentive for partnership participation, with fewer CBP inspections.

Congress recognized the value of the partnership but was concerned about possible vulnerabilities in the program and thus made several adjustments to it in the SAFE Port Act. Included in the law is a requirement that all C-TPAT participants have their security plans validated within one year, each participant show a history of moving goods through the supply chain, and a revalidation process occur no less than once every four years.

CBP has made significant progress, most notably in conducting timely on-site checks or validations of the security measures of C-TPAT members. CBP increased its validations from 133 in 2003, to 3,000 validations in 2007, an increase of 2000%.[56] This success is due to the expansion of the Supply Chain Security Specialists program. CBP anticipates the number of validations and revalidations in 2009 to top 4,000. To address this demand, the SAFE Port Act mandated an increase of 50 security specialists in fiscal year 2008 and again in 2009.

To support the effort to conduct regular and timely validations, the SAFE Port Act requires a pilot program to test the use of a third party to conduct a portion of the validations. In May 2007, CBP submitted a plan to Congress for conducting the pilots, and over the summer announced that 11 contractors were selected to participate. The pilots will focus on supply chains in China, where CBP Supply Chain Security Specialists have been unable to conduct validations. C-TPAT identified 304 member importers that have 75 percent or more of their supply chain in China and which are in Tier 1 status, individually inviting them to participate in the third party validation pilot program that will run until May 1, 2008.[57] However, to date, only seven importers have elected to participate due primarily to the costs they will incur for volunteering for the program. C-TPAT will send notices again in November 2007 and February 2008 to the 304 companies to remind them that C-TPAT is seeking volunteers for the third party validation program in China.[58]

[56] Ibid.
[57] Information provided to Committee Staff by U.S. Customs and Border Protection Legislative Affairs on October 24, 2007.
[58] Ibid.

To ensure that the C-TPAT program continues to be a force multiplier for securing the supply chain:

- ✓ CBP must maintain the ability to conduct timely and quality validations
- ✓ CBP should consider additional benefits for top tier C-TPAT members
- ✓ CBP should develop mechanisms for sharing information on threats and vulnerabilities with C-TPAT members

Enhancing Intelligence & Information Sharing

As with all aspects of homeland security, gathering, analyzing, and disseminating intelligence is critical to the maritime security mission. The jurisdictional complexities and the infinite number of both land and waterside targets in the port environment demand seamless integration and coordination across all federal, state, and local strategies, operations and tactics.

The SAFE Port Act recognizes the critical role of interagency intelligence and information sharing in the efforts to prepare for and prevent a terrorist incident, as well as recover from an incident. The SAFE Port Act authorizes the required funds to facilitate the establishment of interagency operations command centers at all major ports and requires the Secretary to speed up the process by which command center staff receive security clearances. Additionally, the SAFE Port Act requires the Coast Guard to develop a long range vessel tracking system that will feed these operational command centers with an extensive maritime operating picture to ensure the interagency assets have adequate time to respond to inbound waterborne threats.

Long Range Identification and Tracking

"Securing our vast maritime borders depends upon our ability to enhance maritime domain awareness….Identifying threats as far from U.S. shores as possible requires improved awareness of the people, vessels and cargo approaching and moving throughout U.S. ports, coasts and inland waterways."[59]

-Admiral Thad Allen
Commandant, U.S. Coast Guard

[59] Statement of Admiral Thad W. Allen on the President's Fiscal Year 2007 Coast Guard budget before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Fisheries and Coast Guard, June, 15, 2006, https://www.piersystem.com/go/doc/786/120528/

With the release of the National Plan to Achieve Maritime Domain Awareness, President Bush has made maritime intelligence a cornerstone of U.S. port security, and a vital part of our nation's defense:

> There are few areas of greater strategic importance than the maritime domain. The oceans are global thoroughfares that sustain our national prosperity and are vital for our national security. Distinct from other domains (e.g. air and space), the maritime domain provides an expansive pathway through the global commons.[60]

The President clearly stated that the Coast Guard should understand "everything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States."[61] In order to complete this mission, the Coast Guard must be able to effectively locate, identify and track maritime targets of interest not only in U.S. waters, but beyond. In a January 20, 2002 speech, the President said that "accurate information, intelligence, surveillance and reconnaissance of all vessels, cargo and people extending well beyond our traditional maritime boundaries" is central to the United States efforts to achieve domain awareness.[62]

Shortly after September 11, 2001, Congress included a Long Range Identification and Tracking (LRIT) provision in the Maritime Transportation Security Act to monitor suspicious ships outside U.S. waters. However, much like the Transportation Worker Identification Credential provision, LRIT was not implemented. Thus, Congress amended the program in the SAFE Port Act, encouraging DHS to speed up the development and deployment of a LRIT system.

The SAFE Port Act requires the Secretary of Homeland Security to develop and implement a long-range automated vessel tracking system for all vessels in U.S. waters equipped with Global Maritime Distress and Safety System or equivalent satellite technology by April 1, 2007. In an April press release, the Coast Guard claimed it has met this mandate through the use of all-source information. In addition, on October 3, 2007, the Coast Guard released a Notice of Proposed Rulemaking (NPRM) on its Long Range Identification and

---

[60] Bush, George W. *National Strategy for Maritime Security: National Plan to Achieve Maritime Domain Awareness* (Washington D.C.: The White House, October 2005), 2
[61] Ibid.
[62] Ibid.

Tracking (LRIT) program.

However, much still has to be done. At this point the Coast Guard, with support from national technical assets, should be able to locate, identify and track a high priority vessel suspected of carrying a "dirty" bomb or other "clear and present danger." It is not clear that they would be able to identify, track, and analyze daily unreported threats such as small vessels smuggling terrorists, weapons, illegal narcotics and illegal aliens. Also, questions remain as to the effectiveness of the automated identification system (AIS) or the International Maritime Organization's LRIT system as an adequate solution to the long range tracking mandate, since ships can simply disconnect their AIS and LRIT systems if they wish to remain covert.

AIS and LRIT, combined with highly accurate satellite technology and the heightened awareness of commercial mariners, are great tracking tools inside heavily trafficked U.S. territorial waters. However, the 24 nautical mile buffer zone around the U.S. coastline does not provide adequate time to identify, analyze, and respond to an unknown maritime threat, particularly if it is carrying a nuclear, radiological or chemical weapon. The Coast Guard itself has stated that in the maritime environment a "goal line defense" is no defense at all,[63] thus:

- ✓ The Coast Guard must continue to partner with the private sector to identify a better way to establish the common operating picture required by President Bush's National Strategy for Maritime Security.

- ✓ DHS and the Coast Guard must develop policy and procedures for identifying, tracking, and responding to the increasing small vessel threat.

- ✓ The Coast Guard must continue to strengthen its partnerships with maritime information exchanges to supplement its maritime domain awareness resources.

[63] Statement of Rear Admiral David P. Pekoske, Assistant Commandant for Operations on Border Security: Infrastructure, Technology, and the Human Element, before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism, February 13, 2007.

Interagency Operations Centers for Port Security

"Unity of effort requires coordination not only at the apex of the federal government, but also at the tactical level, where response and intervention actions may be taken by diverse authorities, acting independently or in coordination with each other."

-National Strategy for Combating Terrorism

Regional interagency coordination and response plays a major role in the United States' national maritime and counterterrorism strategies.[64] Due to the jurisdictional complexities of America's maritime arena, port security responsibilities are a "shared responsibility that crosses jurisdictional boundaries, with federal, state, and local organizations involved."[65] Regional and local interagency initiatives, such as Project Seahawk in Charleston, South Carolina, serve as the port's focal point for coordination of all federal, state, and local agencies authorized to conduct port and maritime homeland security operations.

The MTSA of 2002 established operating policies for regional port coordination efforts, requiring the Coast Guard to establish Area Maritime Security Committees. As a result, the Coast Guard reorganized its regional command centers into 35 regional Sector Command Centers. In addition, the Coast Guard established a partnership with the Department of Justice, U.S. Navy, and the DHS Office of Science and Technology to create five interagency operations centers in Charleston, Hampton Roads, San Diego, Jacksonville and Seattle to evaluate port and regional-specific network and operational programs.[66]

The SAFE Port Act strengthened these MTSA programs, authorizing $60 million each fiscal year through 2012 and requiring the Secretary to establish an integrated network and command center to enhance intelligence and information sharing, and facilitate operational and tactical preparedness, prevention, and response coordination. In addition, the Act required the Secretary to sponsor the security clearances of appropriate personnel in the command centers.

---

[64] Bush, George W. *National Strategy for Combating Terrorism* (Washington, D.C.: The White House, September 2006), 27.
[65] Caldwell, Stephen L. "Maritime Security: Information-Sharing Efforts Are Improving," Government Accountability Office, July 10, 2006, 5.
[66] Statement of Rear Admiral David P. Pekoske, Assistant Commandant for Operations, U.S. Coast Guard, before the Senate Committee on Commerce, Science and Transportation (CST), October 4, 2007.

The Coast Guard published the mandated report in July, estimating a total cost of $260 million to upgrade 24 high priority Sector Command Centers.[67] Additionally, the Coast Guard is continuing to develop Command 21, a program that seeks to tailor information network systems to the needs of each port's interagency operations command center. The Coast Guard has also joined Customs and Border Protection to identify seven ports "to evaluate joint operations design models.[68]

Interagency operations command centers are the key to tactical preparedness and response. Nobody understands each regional maritime operational theater better than the federal, state, and local personnel assigned to that particular port area. The Government Accountability Office continues to report that the Coast Guard's Area Maritime Security Committees and the interagency operations centers have "fostered cooperation and information-sharing."[69] Congress must appropriate the necessary funding to continue network and systems research and development, stand up the new Coast Guard and CBP pilot projects and ultimately sustain the five existing interagency command centers.

[67] Report to Committee on Homeland Security, July 2007 ***NEED MORE INFO ON REPORT
[68] Statement of Rear Admiral Pekoske, Senate CST, October 4, 2007.
[69] Caldwell, Stephen. "Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports," Government Accountability Office, October 4, 2007.

Conclusion

The SAFE Port Act signed by the President in October 2006 required DHS to implement over 90 different mandates to enhance port and supply chain security, a steep task but one that is incredibly important. Thus far a significant amount of progress has been made to strengthen maritime security and implement the law, but there is still much that has to be done. This report set out to examine some of the key provisions of the SAFE Port Act and encourage the Department to move faster on several unfinished areas.

A few of the items still outstanding are DHS' full rollout of Transportation Worker Identification Cards, improving the Automated Targeting System, and developing a robust vessel tracking capability. At the same time, Congress must maintain its commitment to ensuring resources and authorities are sufficient to carry out mandates. Often, a program that is not adequately funded is as dangerous as no program at all. Legislators should also keep in mind the impact of the laws they write and try to reduce unintended consequences as much as possible. At the committee level, members should continue to evaluate our maritime security needs and craft legislation to address terrorism threats on the horizon.

Everyone involved in the maritime system, from government entities to the private sector, must understand that the terrorist threat we face is very real. Al Qaeda has successfully attacked ships and ports in the past, the *USS Cole* is a well-known example, and experts argue that it's only a matter of time before terrorists exploit the vulnerabilities in our port system and the United States is attacked again.

In testimony before the Senate Homeland Security Committee hearing on post-9/11 threats to the United States, DHS Secretary Michael Chertoff, National Intelligence Director Michael McConnell, John Scott Redd of the National Counterterrorism Center, and FBI Director Robert Mueller described a handful of terrorist threats facing the United States with weapons of mass destruction, small boats laden with explosives, and Islamic radicalization rounding out the top three. With the stakes so high, the SAFE Port Act must be implemented quickly and correctly. We must do all we can to ensure the safety of maritime system and prevent another attack.

Appendix: Quick Reference Guide

DHS	Department of Homeland Security
CBP	Customs and Border Protection
TSA	Transportation Security Administration
MTSA	Maritime Transportation Security Act
AIS	Automated Identification System
AMSC	Area Maritime Security Committees
ATS	Automated Targeting System
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
GAO	Government Accountability Office
LRIT	Long Range Identification and Tracking
PSGP	Port Security Grant Program
SFI	Secure Freight Initiative
TWIC	Transportation Worker Identification Credential