June 14, 2012


Tyler M. Dumler

Available at: https://works.bepress.com/tyler_dumler/2/
# Table of Contents

INTRODUCTION.................................................................................................................1

BACKGROUND..................................................................................................................2

A. The Need for U.S. Maritime Trade Security...............................................................2

B. Container Security Initiative......................................................................................4

C. Customs-Trade Partnership Against Terrorism........................................................10

D. The 24-Hour Rule .....................................................................................................13

E. International Ship and Port Facility Security Code....................................................15

F. Secure Freight Initiative ............................................................................................18

ARGUMENT......................................................................................................................20

A. 100 Percent Scanning Under SFI is Unrealistic.........................................................20

B. CSI Should be Expanding Instead of Shrinking or Remaining Stagnant..................21

C. CBP Should Continue Developing Technological Adaptations to Address
   Setbacks.......................................................................................................................24

D. Trade Security Must Prevail in the Short-Term in Order for Global Trade to
   Prevail in the Long-Term............................................................................................26

E. The Perceived Lack of Reciprocity............................................................................28

F. C-TPAT Adequately Addresses the Problem of Containers Being
   Loaded Before Reaching Ports..................................................................................30

G. CBP’s Layered Security Strategy Has Effectively “Pushed the Borders
   Outward” in the Short-Term and Will Enhance Global Trade in the Long-Term........31

CONCLUSION ..................................................................................................................33

Bibliography ....................................................................................................................35
The Container Security Initiative:

A Layered Security Strategy for Securing

Containerized Cargo

Tyler Dumler

April 24, 2012
I. INTRODUCTION

On September 11, 2001, the United States fell victim to a set of orchestrated terrorist attacks including the destruction of the World Trade Center in New York City — a symbol of free trade. With the perceived threat of a possible future attack on trade, the U.S. undertook the mission of securing its channels of world trade. Government officials and security experts recognized the vulnerability of maritime shipping ports even before the events of 9/11 due to their size, ease of access by land and sea, proximity to urban areas, and the large amount of cargo they handle. The destruction of the World Trade Center did nothing to alleviate these concerns. Among the fallout from the attacks on 9/11 was an elevated focus on the security risks to channels of world trade.

The Department of Homeland Security (DHS) was established in 2002 with a core purpose of preventing terrorists and their instruments from entering the United States by securing all national borders, including ports and sea transportation systems. Under DHS’s direction, the Bureau for Customs and Border Protection (CBP) and the United States Coast guard are charged with the responsibility of administering port and container security. CBP has taken the lead role in maritime security and is entrusted with the responsibility of ensuring the security of shipping containers entering the United States.

---

1 See R. V. G. CLARKE & GRAEME R. NEWMAN, OUTSMARTING THE TERRORISTS 94 (Greenwood Publ’g Grp. 2006).
2 JOHN F. FRITTELLI ET AL., PORT AND MARITIME SECURITY: BACKGROUND AND ISSUES 1–2 (Susan Boriotti et al. eds., 2003).
4 Id. at 357.
6 Hoverter, supra note 3, at 362.
In order to satisfy its responsibilities, DHS has instituted a layered security strategy. A layered defense provides multiple and interconnected security layers to most efficiently protect against security risks. The building blocks of this layered security approach include the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), the 24-Hour Rule, the Automated Targeting System (ATS), and the International Ship and Port Facility Security (ISPS) Code adopted by the International Maritime Organization (IMO) at the strong suggestion of the U.S. Coast Guard. These layered security programs are part of U.S. efforts to push its borders outward.

CSI, along with the other building blocks of CBP’s layered security strategy, should be bolstered to increase trade security in the short-term and enhance global trade in the long-term. These building blocks will be explained in Part Two before moving on to discuss the future of U.S. maritime trade security in Part Three.

II. BACKGROUND

A. The Need for U.S. Maritime Trade Security

Although exact estimates vary, studies tend to agree that over 90 percent of all

7 It should be noted CBP’s approach is attributable to DHS as an agency of the larger department. Future references to CBP and DHS will assume a uniform mission unless explicitly stated otherwise. This mention is only to clarify and avoid inadvertently implying that DHS and CBP are operating under adverse missions.


10 Grillot et al., supra note 8, at 68.
goods in the world move by container.\textsuperscript{11} U.S. trade accounts for 10 percent of the world container traffic.\textsuperscript{12} Sea vessels are the general mode of transport when moving containers.\textsuperscript{13} Over 11 million shipping containers consistently enter U.S. seaports annually.\textsuperscript{14} The Department of Transportation estimates that U.S. container traffic will increase by 50 percent between 2001 and 2020, and international container traffic is expected to more than double in that time.\textsuperscript{15} 

The U.S. has about 7,000 miles of land border and 95,000 miles of shoreline, so it is understandable for port security to be a major concern when dealing with the nation’s general security.\textsuperscript{16} However, trade security was not regarded as a major concern prior to 2001 because there had been relatively few high-profile security problems.\textsuperscript{17} Trade volumes continued to rise and the percentage of container inspections conversely continued to decline in the latter years of the twentieth century.\textsuperscript{18} By 2001, less than two percent of the several million containers shipped to the U.S. annually were physically

\begin{itemize}
  \item \textsuperscript{12} GRILLOT ET AL., \textit{supra} note 8, at 68.
  \item \textsuperscript{13} See Id.
  \item \textsuperscript{15} North, \textit{supra} note 11, at 194.
  \item \textsuperscript{16} GRILLOT ET AL., \textit{supra} note 8, at 4.
  \item \textsuperscript{18} Id.
\end{itemize}
inspected by U.S. customs. The events of 9/11 ushered in a new perspective regarding trade security. The detonation of a single nuclear device at a port could result in up to $1 trillion dollars in damage. Due to the perceived importance and vulnerabilities of ports after 9/11, it was clear that efforts needed to be taken to increase port and container security.

**B. Container Security Initiative**

“‘CSI has become one of the most influential maritime security initiatives in the world.’” It makes sense, then, to begin by discussing this building block of the layered security strategy implemented by CBP. CBP launched CSI in January 2002, very shortly after the agency’s creation. CSI was later made permanent by the Security and Accountability for Every Port (SAFE Port) Act of 2006. The adoption of this security initiative by CBP is reflective of the agency’s restructuring immediately after 9/11. While the Customs Service, CBP’s predecessor agency, had previously been part of the Treasury Department, the agency was revamped into CBP under DHS following 9/11.

---

19 Id. at 199.
20 North, supra note 11, at 194.
21 Supra note 2 and accompanying text.
This structural change is reflected by CBP’s newfound focus on security.

There are four core elements of CSI. First, identify high-risk containers based on ATS, the size of the container, and the port of origin. All information about cargo is reviewed and given a risk evaluation under the ATS. Second, pre-screen and evaluate containers at their port of departure prior to shipment. Third, use technology to efficiently and quickly screen containers that have been identified as high-risk. Fourth,


use smarter, more secure containers that are tamper evident. Figure 1, above, is a visual illustration explaining CSI’s screening process.28

There are currently 58 CSI ports, accounting for over 80 percent of containerized cargo bound for the U.S.29 Nineteen of the twenty largest ports in the world are included in these 58 CSI ports.30 All foreign ports are eligible for eventual CSI membership.31 CSI ports are established through bilateral agreements between the U.S. Department of State and the customs agencies of foreign governments.32 CSI requires the partnering foreign government to enhance its development and implementation of advanced screening techniques, agree to oversight from CBP agents stationed at the foreign country’s port, and requires foreign customs agents to share information with U.S. officials.33 In exchange, the foreign CSI port is given the option of stationing their agents at U.S. ports and receives expedited processing at the destination port due to the enhanced security clearance of the port of origin.34

These bilateral agreements are less intrusive means of extending U.S. policy to international maritime trade than unilateral enforcement of similar measures.35 Any loss of sovereignty or increased assertion of U.S. jurisdiction is legally justifiable because the

28 Skinner, supra note 24, at 1.
30 Holmes, supra note 26, at 15.
31 SUZETTE R. GRILLOT ET AL., PROTECTING OUR PORTS: DOMESTIC AND INTERNATIONAL POLITICS OF CONTAINERIZED FREIGHT SECURITY 79 (Ashgate Publ’g Grp. 2010).
32 Id. at 70.
33 Id. at 79.
34 Maney, supra note 26, at 325.
foreign countries are consenting to these bilateral agreements. In actual practice, perhaps the most legitimization of CSI came from its eventual international recognition and support rather than this theory of consent. The agreement reached with the Netherlands in 2002 for Europe’s largest seaport, Rotterdam, to become a CSI port resulted in a domino effect giving legitimacy to CSI.

While initially outraged at CSI’s approach of dealing with each member country of the European Union (EU) rather than the EU as a whole, the EU eventually came around to be one of the strongest supporters of CSI along with the World Customs Organization (WCO) and Group of Eight (G8). This substantial multilateral support through the EU, WCO, and G8 has essentially internationalized and legitimized CSI and substantially reduced doubt as to the legality of the initiative’s expansive nature extending beyond the geographic borders of the U.S.

CSI relies strongly upon the cooperation of foreign governments. Reciprocity is instrumental to the success of CSI. While CBP personnel can access shipment information and act in an advisory capacity while identifying high-risk containers, the foreign host governments retain final say regarding whether, when, and how high-risk containers are inspected. In theory, the most beneficial aspect of becoming a CSI port

_________________________
37 GRILLOT ET AL., supra note 31, at 79.
38 Id. at 110.
39 Bowman, supra note 36, at 207.
40 Id. at 227.
42 Bowman, supra note 36, at 205.
is that it allows the foreign country, in exchange, to station personnel at U.S. ports. The economic incentive of expedited shipments upon reaching the U.S. is a bonus to the reciprocity aspect. Whether this is the reality will be discussed in Part Three.

There are many criticisms of CSI. One criticism is that CBP relies primarily on the shipper’s own documentation to analyze the risk of a container. Shippers load the majority of containers at their own facilities outside the supervision of both CBP and foreign port authorities. If a shipper intends to smuggle goods, individuals, or weapons by means of a shipping container, it seems reasonable to conclude that such an entity would be willing to inaccurately describe the contents of its containers on the manifest. Placing too much emphasis on the shipper’s manifest risks ineffectively analyzing which containers are high-risk.

Another problem with CSI is the burdensome delays created by container inspections. “It takes five agents three hours to conduct a thorough inspection of a single container.” “Being directed to routinely locate and remove U.S.-bound boxes from their stacks shortly before scheduled loading can be enormously disruptive to yard operations.” The incentive for the foreign port created by this risk of delay is counter-

---

43 Maney, supra note 41, at 325.
44 Id.
45 Id. at 326.
46 Id.
intuitive. Foreign ports and shippers are motivated to not provide information that would identify a container as high-risk, because doing so leads to economically detrimental delays.\footnote{Id.}

A third problem with CSI is CBP’s lack of resources.\footnote{Rossella Brevetti, Customs: GAO Finds Hurdles to CBP’s Implementation of Port, Cargo Security Programs, INTERNATIONAL TRADE REPORTER: NEWS ARCHIVE, May 3, 2007, http://news.bna.com.www2.lib.ku.edu:2048/itln/ITLNWB/split_display.adp?fedfid=7258865\&vname=itrnotalissues&wsn=516498000&searchid=17219244&doctypeid=1&mode=date&split=0&scm=ITLNWB&pg=0.} Targeting and identifying high-risk containers becomes difficult without sufficient staff.\footnote{Odoyo, supra note 47, at 260 (quoting Marjorie Florestal, Terror on the High Seas: the Trade and Development Implications of U.S. National Security Measures, 72 BROOK. L. REV. 385, 388 (2007)).} As mentioned, it took five agents three hours to conduct a thorough inspection of a single container in 2007. At this rate, it would have taken six months for port officials to inspect one day’s shipments of containers to the U.S.\footnote{Brevetti, Customs: GAO Finds Hurdles to CBP’s Implementation of Port, Cargo Security Programs, supra note 50.} Additionally, CSI was unable to ensure that containers identified as high-risk would ever be inspected in 2007.\footnote{Jennifer L. North, The Ins and Outs of Modern Ports: Rethinking Container Security, 5 S.C. J. INT’L L. & BUS. 191, 205 (2009). (quoting Container Security: Hearing Before the Subcomm. on Homeland Security of the H. Comm. on Appropriations, 111th Cong. (2009) (statement of Charles R. Gallaway, Acting Director, Domestic Nuclear Detection Office)).} Technology available in 2009 was incapable of distinguishing between threatening materials and naturally occurring radioactive material, like kitty litter and ceramic tile.\footnote{See Id.} Without sufficient resources, CBP is unable to bolster the number of CSI officials and improve technological inspection capabilities to decrease the amount of time necessary to identify and inspect high-risk
containerized cargo.

It is also argued that CSI has increased the gap between developed countries and developing or least-developed countries.\textsuperscript{55} Many of these poorer developing countries lack the resources and technical know-how to implement CSI’s requirements.\textsuperscript{56} This issue will be discussed more in Part Three along with shared complaints by Europe and Asia regarding CSI’s failure to recognize that all ports are not similar in structure and operation.

It must be remembered that CSI, along with the governing bodies of CBP and DHS, are relatively infantile in the grand scheme of international trade. While there is certainly room for improvement and further development, there should be hesitance before contemplating the abandonment of CSI.

\textbf{C. Customs-Trade Partnership Against Terrorism}

The second building block of CBP’s layered security strategy, the Customs-Trade Partnership Against Terrorism (C-TPAT), was similarly created in 2002 under the guidance of CBP.\textsuperscript{57} C-TPAT seeks to move the borders even further outward than CSI.\textsuperscript{58} Like CSI, C-TPAT was codified in 2006 under the SAFE Port Act.\textsuperscript{59} By 2007, “C-TPAT had become the largest ‘voluntary’ partnership between private businesses and the U.S. government, with over 5,600 certified companies and over 10,000 pending applications.\textsuperscript{60} This number has since increased to over 10,000 members in 2011 with a goal to boost

\textsuperscript{55} Odoyo, \textit{supra} note 47, at 262.
\textsuperscript{56} Id.
\textsuperscript{57} North, \textit{supra} note 54, at 199.
\textsuperscript{58} Id.
\textsuperscript{59} Id.
\textsuperscript{60} Odoyo, \textit{supra} note 47, at 263.
membership to 40,000 by 2016.\textsuperscript{61} While C-TPAT has received more attention than CSI, as can be seen by the focus on its expansion while CSI remains stagnant, this initiative shares CSI’s directives and serves as a coordinated effort to secure freight beyond U.S. ports of entry.\textsuperscript{62}

C-TPAT is a voluntary agreement between DHS and private firms in the global supply chain including importers, brokers, forwarders, air/sea/land carriers, contract logistics providers, warehouse operators, and manufacturers where the private entities agree to provide additional information regarding the contents of their shipments and commit to C-TPAT security recommendations.\textsuperscript{63} The criteria for participating in C-TPAT are extensive.\textsuperscript{64} Firms must conduct a self-assessment of their security practices using U.S. guidelines, submit a security profile of their supply chains to CBP, develop a security plan that incorporates C-TPAT guidelines, and work towards building C-TPAT guidelines into their relationships with other firms in the global supply chain.\textsuperscript{65} Companies can only qualify for C-TPAT if their \textit{entire} supply chain qualifies.\textsuperscript{66}

Once a private firm qualifies and partners under C-TPAT, the entities are able to

\textsuperscript{62} SUZETTE R. GRIJLLOT ET AL., \textsc{Protecting Our Ports: Domestic and International Politics of Containerized Freight Security} 77 (Ashgate Publ’g Grp. 2010).
\textsuperscript{63} Odoyo, \textit{supra} note 47, at 264.
\textsuperscript{64} Id.
\textsuperscript{66} Odoyo, \textit{supra} note 47, at 264.
apply for validation in three tiers. The benefits and security level of the partnered entity increase as they move from tiers one through three, respectively.

Tier 1 status will include a background investigation and extensive documentation review by CBP. The benefits to the Tier 1 status allow a reduction in the risk score assigned by ATS. Tier 2 status involves those satisfactory Tier 1 participants whose security practices are assessed onsite by the Department [of Homeland Security]. This assessment conducted at foreign locations should be completed within one year of Tier 1 validation. Tier 2 benefits include reduced risk scores in ATS, reduced examinations of cargo, and priority searches of cargo. Tier 3 participants receive additional benefits beyond tier 2 status. Tier 3 participants are those who have demonstrated a sustained commitment to maintaining satisfactory security measures exceeding those of the Tier 2 entity. . . . Incentives to become Tier 3 participants include expedited release of a cargo in destination within the US (sic) during all threat levels, further reduction in examinations of cargo, further reduction in the risk score assigned pursuant to ATS, and inclusion in joint incident management exercises.

A common criticism of C-TPAT is that it runs afoul of GATT MFN treatment. However, C-TPAT calls for differential treatment between private companies rather than between member countries. Because C-TPAT involves agreements between private entities and not governmental bodies, the CBP initiative does not run afoul of GATT requiring MFN treatment to all WTO members. As with other security measures, it is additionally argued that C-TPAT interferes with free trade. The classical concepts of complete sovereignty are less absolute in a globalizing society within the context of terrorism and public security. Private entities are no longer excluded from formulation

---

68 Id. at 200–01.
69 Odoyo, supra note 47, at 265.
and implementation of security policies.\textsuperscript{71} Even though such thought seems at odds considering it is the U.S. implementing security policies which may interfere with free trade, in cases of conflict, public security should take precedence over free trade and transport.\textsuperscript{72}

D. The 24-Hour Rule

The third building block of CBP’s layered security strategy is the Advance Manifest Regulation, more commonly known as the “24-Hour Rule.”\textsuperscript{73} The 24-Hour Rule also finds its genesis in 2002, but it did not become effective until 2003.\textsuperscript{74} Although the 24-Hour Rule is generally placed under the care of CBP,\textsuperscript{75} it is understandable why some commentators would classify the 24-Hour Rule as a security measure of the U.S. Coast Guard.\textsuperscript{76} Conveyance of detailed information under the 24-Hour Rule notifies the U.S. Coast Guard of whether unauthorized cargo is aboard the ship and allows interception prior to the ship’s entry into port.\textsuperscript{77} With this understanding of the logistics, it is now possible to understand the substance of the 24-Hour Rule.

The 24-Hour Rule requires that “manifests listing the contents of containers must be submitted to federal officials 24 hours before those containers are \textit{loaded} onto ships

\textsuperscript{71} Id.
\textsuperscript{72} Id.
\textsuperscript{75} See e.g. Id.; Hoverter, supra note 73, at 363; SUZETTE R. GRILLOT ET AL., \textit{PROTECTING OUR PORTS: DOMESTIC AND INTERNATIONAL POLITICS OF CONTAINERIZED FREIGHT SECURITY} 78 (Ashgate Publ‘g Grp. 2010).
\textsuperscript{77} Id. at 265.
bound for U.S. ports.” Before the 24-Hour Rule, ships only had to carry the manifest on board and U.S. customs officials would inspect the manifest upon arrival at the U.S. port. Manifests only had to be submitted 48 hours prior to the vessel’s arrival at the U.S. port. This allowed carriers to fill out the vessel’s manifest en route to the U.S. and did not interfere with the carrier’s ability to load “just-in-time” shipments. Failure to comply with the 24-Hour Rule can result in both civil and criminal penalties, including a “Do Not Load” message. Carriers subject to a “Do Not Load” message can incur millions of dollars in economic loss due to the denial of entry to the U.S. port and, in turn, the delayed delivery of goods. Should inventory be delayed entry, the repercussions could cost the importer millions of dollars.

Although the 24-Hour Rule has been called “one of the most controversial security related regulations,” it has not received as much legal criticism as C-TPAT. The lack of challenges under international law is likely due to the equal application of the 24-Hour Rule to all carriers, precluding the argument that some carriers are receiving preferential treatment. The largest criticism of the 24-Hour Rule is its cause of delay

79 Id.
80 Id.
81 Id. at 265–66.
82 Id. at 267.
83 See Id.
85 Odoyo, supra note 76, at 266.
86 Id.
and restrictive effect on last minute cargo. Because the 24-Hour Rule requires manifests listing the contents of containers to be submitted to federal officials 24 hours before those containers are loaded onto ships bound for U.S. ports, so-called “just-in-time” shipments of containers must either be turned away or, if the value of the just-in-time containers warrants waiting, result in the delay of the vessel’s departure. Just-in-time shipments are not the only containers causing lost time and money under the 24-Hour Rule. Storage costs at the port of origin increase due to the lost time and money from the 24-hour waiting period before any shipments can be loaded onto a vessel.

E. International Ship and Port Facility Security Code

The International Ship and Port Facility Security (ISPS) Code was implemented by the International Maritime Organization (IMO) and entered into force in 2004. The IMO adopted the ISPS Code as amendments to the International Convention for the Safety of Life at Sea (SOLAS) after the U.S. Coast Guard advocated for such changes. Rather than introducing ISPS as an independent directive, offering the Code as amendments to an existing directive allowed the IMO to streamline its passage. This was the result of significant influence and lobbying by the U.S.

“The ISPS Code sets forth mandatory security requirements that must be taken by governments, ports, shipping companies, and terminal operators to enhance the security

87 Id.
88 Id.
89 Id.
90 Id. at 268
92 SUZETTE R. GRILLOT ET AL., PROTECTING OUR PORTS: DOMESTIC AND INTERNATIONAL POLITICS OF CONTAINERIZED FREIGHT SECURITY 79–80 (Ashgate Publ’g Grp. 2010).
93 Id. at 79.
of the world’s maritime transportation system.” Compliance with the ISPS Code is mandatory for 148 contracting parties. The consequences of failing to comply or failing to maintain compliance with the IMO’s maritime security measures are said to be “serious and far reaching.” The ISPS Code has been criticized for having no real effect due to the non-binding nature of IMO policies. The IMO merely promotes improvements by member governments and the maritime industry. However, U.S. Coast Guard personnel work closely with member governments and the IMO to ensure ISPS standards are truly being met. These Coast Guard personnel are referred to as International Port Security Liaison Officers (IPSLO). If a port or ship is determined by an IPSLO to not be in compliance with ISPS requirements, then goods going to the Unites States or other foreign ports may be delayed by the U.S. Coast Guard. The U.S. Coast Guard’s backing of IMO gives ISPS teeth.

The ISPS Code seeks to strengthen port security measures by assessing both the security threat of port facilities as well as the ship security of each vessel in a carrier’s fleet. ISPS institutes three levels of security preparedness depending upon perceived threat. Fencing, lighting, cameras, and securing personnel entering and leaving ISPS

---

95 Odoyo, supra note 76, at 268.
96 Id.
97 Id.
99 GRILLOT ET AL., supra note 92, at 80.
100 Id.
101 Id.
102 GRILLOT ET AL., supra note 92, at 80.
areas of a seaport are requirements at the initial level.\textsuperscript{103} Ships similarly must meet minimum security standards.\textsuperscript{104} The increase in security restrictions under ISPS coincide with the increase in security threats.\textsuperscript{105}

The IMO has also been cited for having a poor record of taking swift and effective action when faced with international security concerns.\textsuperscript{106} The Achille Lauro incident in the 1980s is an example of how maritime safety and security issues have been dealt with by the IMO.\textsuperscript{107} In response to the Achille Lauro incident, the IMO immediately voiced its concern about the unlawful acts threatening the safety and security of ships and their passengers.\textsuperscript{108} However, it took almost a decade before a legal framework was created to deal with these concerns.\textsuperscript{109} Perhaps this criticism of the IMO engaging in rhetoric when faced with international security concerns without implementing swift and effective action can be dispelled in the context of ISPS. Unlike the Achille Lauro incident, the IMO streamlined passage of ISPS in 2002 shortly after the events on 9/11 which led to international security concerns — attacks which, notably, did not directly involve maritime transportation.\textsuperscript{110} An optimistic conclusion would be that the IMO has become more responsive to international security concerns in recent decades and criticism of the organization’s unresponsive nature is no longer warranted.

\begin{footnotesize}
\begin{footnotes}
\textsuperscript{103} Id.
\textsuperscript{104} Id.
\textsuperscript{105} Id.
\textsuperscript{107} Id. at 138–39; The Achille Lauro incident involved the hijacking of an Italian cruise liner by members of the Palestinian Liberation Front.
\textsuperscript{108} Id. at 139.
\textsuperscript{109} Id.
\textsuperscript{110} See GRILLOT ET AL., supra note 92, at 80.
\end{footnotes}
\end{footnotesize}
F. Secure Freight Initiative

It is almost impossible to discuss port and container security today without mention of the Secure Freight Initiative (SFI). Of all U.S. container security policies, SFI is, by far, the largest point of global contention. This initiative’s mandated 100 percent scanning of all goods coming from foreign ports destined for the U.S. is criticized for being unattainable. Some critics argue the U.S. is using SFI as a form of protectionism to limit imports in order to increase sales of domestic goods. SFI was established in 2007 “to test the feasibility of moving from a risk-based approach to 100% scanning of all cargo containers bound for U.S. ports” by 2012. As the July 12, 2012 deadline quickly approaches, only about 4 to 5 percent of the eleven million cargo containers are currently being scanned. Many port officials believe that the initial post-9/11 security measures, including CSI, C-TPAT, and ISPS, created a secure environment at their seaports and initiatives beyond these, like SFI, are superfluous and provide diminishing returns. In 2009, DHS Secretary Janet Napolitano estimated that meeting the July 12, 2012 deadline would cost $8 million for each of the 21,000 shipping lanes at more than

111 Id. at 83.
112 Id. at 84.
115 GRILLOT ET AL., supra note 95, at 83.
700 ports shipping cargo into the U.S.\textsuperscript{116} This 100 percent scanning approach, compared with the risk-based alternative currently in place, presents huge costs in implementation, training, installation of scanning equipment, and the eventual delay in shipments resulting from a drastic increase in the percentage of containers being scanned.\textsuperscript{117} Developing and least-developed countries unable to absorb the costs of personnel and technology required for 100 percent scanning will be forced to ship goods bound for the U.S. through a third country’s port.\textsuperscript{118} This transshipment of goods will result in higher shipping costs and does not promote development.\textsuperscript{119}

SFI has been deemed impractical for multiple reasons. Scanning the enormous volume of individual containers prior to leaving a foreign port would be nearly impossible.\textsuperscript{120} The risk of the doomsday scenario, though catastrophic, is actually quite low, so the exceptional cost of SFI exceeds the perceived benefits of the initiative.\textsuperscript{121} Finally, shielded nuclear materials would still go unnoticed even if 100 percent scanning were achieved using scanning equipment available in 2009.\textsuperscript{122}

The SAFE Port Reauthorization Act of 2011 would eliminate SFI if DHS certifies the current, multi-layered security strategy as sufficiently effective.\textsuperscript{123}

\begin{thebibliography}{99}
\bibitem{116} Brevetti, \textit{Customs: Nadler Criticizes DHS’ Inability to Meet 100 Percent Sea Cargo Scanning Mandate}, supra note 120.
\bibitem{119} Id. at 140.
\bibitem{120} North, supra note 123, at 202.
\bibitem{121} Id.
\bibitem{122} Id.
\end{thebibliography}
SFI’s 100 percent scanning requirement seems to have been tested and found to be impractical. However, the SAFE Port Reauthorization Act of 2011 does not appear to have gained much traction and looks to have a low likelihood of being enacted by Congress.124 “Despite the limitations discussed before Congress, it appears that most lawmakers disagree with the expert assessments of detection capabilities or simply demand more protection capability than is currently available.”125

III. ARGUMENT

A. 100 Percent Scanning Under SFI is Unrealistic

Only 4 to 5 percent of containers entering the U.S. are currently scanned.126 This, clearly, is nowhere near the July 12, 2012 goal of 100 percent. In fact, only 86 percent of containers exiting foreign ports were pre-screened by CBP in 2009.127 This pre-screening is the mere process of identifying high-risk containers to be flagged for further scrutiny.128 It is unrealistic to expect 100 percent scanning when 100 percent screening has not been accomplished.

DHS has been criticized for neither making a realistic effort to implement the 100

125 North, supra note 123, at 205.
127 North, supra note 123, at 197.
128 Id.
percent scanning mandate nor offering an alternative proposal to achieve the same ends. This criticism, however, is somewhat misguided. DHS has at least made efforts to test the feasibility of SFI by designating Puerto Cortes, Singapore, and Busan (Pusan) as SFI ports. Although DHS does not appear to have presented a formal assessment of SFI’s lack of feasibility, the astronomical costs — both in implementation and in effect — as well as the failure to meet the 100 percent scanning goal allow the reasonable conclusion that SFI has failed the test of feasibility. A formal presentation of DHS’s findings from its three SFI test ports should be presented on this matter. However, to say DHS has failed to offer an alternative proposal to achieve the same ends is inaccurate. DHS Assistant Secretary David Heyman and Kevin McAleenan of the CBP both testified that the layered security strategy consisting of the building blocks discussed in Part Two is a better alternative to 100 percent scanning. This risk-based approach allows DHS to focus on high-risk cargo without disrupting the flow of commerce.

B. CSI Should be Expanding Instead of Shrinking or Remaining Stagnant

CBP has no plan of expanding CSI beyond the current 58 operational CSI ports. This lack of intent to expand CSI can be seen from the stagnant number of CSI

---

129 Brevetti, Customs: Nadler Criticizes DHS’ Inability to Meet 100 Percent Sea Cargo Scanning Mandate, supra note 132.
131 Brevetti, Customs: Nadler Criticizes DHS’ Inability to Meet 100 Percent Sea Cargo Scanning Mandate, supra note 132.
132 Id.
ports remaining at 58 since 2007.\textsuperscript{134} In fact, the number of CSI ports dipped to 53 in 2009 due to an overall decrease in worldwide cargo resulting from global economic struggles.\textsuperscript{135} Between 2009 and 2011 the number of CSI officers at foreign ports decreased from 167 to 79.\textsuperscript{136} The number of CSI ports and officers should be increased. Since DHS is not fully committed to SFI, for good reason, alternative maritime security measures must be pursued. C-TPAT has continued its exponential expansion while CSI has remained stagnant.\textsuperscript{137} While CBP should maintain its commitment to C-TPAT, the focus on profiling private entities should not wholly consume the more grounded individual container risk assessments under CSI. CSI, along with the other building blocks of DHS’s layered security strategy, should be bolstered to increase trade security in the short-term and enhance global trade in the long-term.

The “10 + 2” rule is being developed as part of CBP’s layered security strategy

\textsuperscript{135} Skinner, Supra note 140, at 1.; This decrease was only temporary and the number of CSI ports has since returned to 58.
\textsuperscript{136} Brevetti, Customs: Nadler Criticizes DHS’ Inability to Meet 100 Percent Sea Cargo Scanning Mandate, supra note 132.
and bolsters the risk-based security strategy of DHS. This rule requires “U.S. importers or cargo owners to file 10 additional data elements with CBP 24 hours prior to vessel loading. Further, it would require ocean carriers to provide vessel stowage plans prior to U.S. arrival and copies of electronic container status messages.” By adding these additional criteria for risk-assessment, CBP is actually attempting to expand its layered security strategy as an alternative to SFI. Adoption of the “10 + 2” rule would expand upon CSI’s first core element by enhancing CBP’s ability to identify high-risk containers.

Although the costs of expanding CSI and obtaining additional scanning equipment and personnel with technical know-how to make the most of advanced security techniques seem astronomical, they must be evaluated relative to the security concerns being contemplated. One estimate shows the cost of installing cargo-scanning equipment at every marine container terminal in the world, allowing a 90 percent detection rate of shielded nuclear materials, would be approximately $500 to $600 million. This cost is equal to the price of four new F-22 fighters. Similarly, a

---


140 THOMAS PRESTON, FROM LAMBS TO LIONS: FUTURE SECURITY RELATIONSHIPS IN A WORLD OF BIOLOGICAL AND NUCLEAR WEAPONS 362 (2007).

141 Id.
smarter container equipped with sensors and tracking equipment certified at its origin would add only 1.5 percent to average overseas shipping costs.142 When compared with the repercussions of a potential security breach, these costs begin to seem far less drastic.

C. CBP Should Continue Developing Technological Adaptations to Address Setbacks

The remaining three core elements of CSI also have room for improvement. In large part, these improvements will come in the form of technological advances. Improving pre-screening and evaluation of containers to 100 percent at ports of departure prior to shipment may be more easily accomplished by increasing the number of CSI personnel and improving container scanning equipment. A larger body of CSI personnel will be more able to thoroughly and efficiently review containers at the screening stage and improved scanning equipment will increase CBP’s ability to effectively recognize high-risk containers. Satisfaction of the third core element of screening containers identified as high risk will coincide with this increase in personnel and scanning technology. Finally, CBP must be granted time to develop smarter containers which will become the standard for future containerized trade.

DHS, CBP, and the initiatives under these institutions are all relatively young. CSI, along with other building blocks of layered security have, at most, been in existence for just over a decade.143 It is no surprise, then, that problems have arose when implementing these security initiatives. Port officials in Europe and Asia have expressed criticism regarding CSI’s failure to recognize that all ports are not similar in structure and

142 Id.
Some ports rely more heavily on rail and truck transport while others depend primarily upon barges for shipments of containers. The scanning infrastructure will vary depending on the mode of delivery relied upon by the port. CBP must recognize this variation when implementing regulations under CSI. Instead of having a single, uniform standard for all CSI ports, CBP should investigate and determine the appropriate security procedures and regulations for different models of ports with shared shipping characteristics.

Other ports, even though they may be willing and financially able to comply with CSI requirements, simply lack the ability to expand. Examples of ports logistically incapable of expansion include ports in densely populated urban areas where land is scarce or the Port of Antwerp in Belgium along a river and backed up to its national border with The Netherlands. In these situations, CSI must consider unique security procedures and regulations related to the possible adoption of an alternative port model similar to that adopted by Singapore — relying more heavily on offshore loading and unloading operations.

The Automated Commercial Environment (ACE) is an example of CBP’s ability to adapt technologically to the evolving needs of trade security. ACE was developed in 2009 to replace the manifests being used at the time. ACE account owners are able to

144 SUZETTE R. GRILLOT ET AL., PROTECTING OUR PORTS: DOMESTIC AND INTERNATIONAL POLITICS OF CONTAINERIZED FREIGHT SECURITY 81 (Ashgate Publ’g Grp. 2010).
145 Id.
146 Id.
147 Id. at 83.
148 Id.
149 See Id.
complete many functions electronically that previously required a telephone call or e-mail to CBP. These automated functions include checking bill of lading status, confirming CBP receipt of manifest data, adding or changing vessel codes, and identifying authorized or unauthorized custodial bond users. These functions serve to enhance “identification of shipments that may pose a risk and expedite the prearrival processing of legitimate cargo.” ACE is an example of technological enhancements designed to increase coordination between the multiple security layers by compiling and increasing the amount of data shared between agencies while at the same time eliminating redundant paper processing by shifting to alternative electronic means.

D. Trade Security Must Prevail in the Short-Term in Order for Global Trade to Prevail in the Long-Term

“For economies to prosper and trade to flourish, security is a precondition.” Securing international trade is a collaborative effort. “The International threat of terrorism requires global action, collaboration[,] and innovation to ensure our mutual security and defend against terrorists.” Coordination and cooperation are required for

151 Id.
152 Id.
153 Id.
154 Id.
156 Customs: Napolitano Tours Barcelona CSI Port, INTERNATIONAL TRADE REPORTER: NEWS ARCHIVE, Apr. 15, 2010, available at
uniform compliance of security measures. Without uniform compliance, the weaker ports become attractive targets for terrorists.\textsuperscript{157}

A major problem with uniform compliance is the inability of some ports to afford the implementation of technology and experienced personnel required by security initiatives.\textsuperscript{158} Currently, the foreign host country is expected to bear the cost of nonintrusive nuclear and radiological detection equipment.\textsuperscript{159} An alternative to this approach is for the U.S. to provide capacity-building assistance similar to that offered in the Secure Trade in the APEC Region (STAR) initiative.\textsuperscript{160} Capacity-building assistance from the U.S. to qualifying ports in developing and least-developed countries would address the concern that some ports are financially unable to implement adequate security measures. By assisting the less financially adept ports in implementing adequate security measures, uniform compliance will more likely be achieved. The result will be a positive step towards securing containerized maritime cargo because the number of susceptible ports will, in turn, decrease.

\textsuperscript{158} Suzette R. Grillot et al., \textit{Protecting Our Ports: Domestic and International Politics of Containerized Freight Security} 83 (Ashgate Publ’g Grp. 2010).
The terrorist attacks on 9/11 were intended to disrupt world trade. This is illustrated by the targeting of the World Trade Center, a symbolic hub of world trade. It has been argued that the resulting laws promoting security at the expense of free trade illustrates that the terrorists are winning. However, economics and trade function in a context. Neither absolute security at the complete expense of free trade nor free trade with no security are sustainable options. Security is a precondition in order for underlying international economic and trade development to occur. Security measures may not directly solve the underlying problems which lead to terrorism, but they may serve as a prerequisite for fixing the underlying problems.

E. The Perceived Lack of Reciprocity

The key to CSI’s success is reciprocity. Reciprocity is intended to be the main incentive for foreign ports to enter bilateral agreements with the U.S. to become a CSI port. Expedited processing of goods at the destination port is considered a reward of participation and not the primary purpose of participation. There is evidence of a

---

162 Id.
163 Id.
166 Id.
167 Id.
perceived lack of reciprocity by the U.S. under CSI. In 2006, only Canada and Japan had stationed customs personnel in the U.S. under the CSI program. If reciprocity truly is the key to success, the U.S. must be willing to extend the same genuine offer of participation to foreign officials at U.S. ports as is expected to be offered by foreign ports to U.S. officials. Enhanced reciprocity would mean that the U.S. would also be willing to scan the millions of full and empty containers that it ships abroad.

Although reciprocity is certainly a key to the legitimacy and success of CSI, the idea that it is the primary reason for becoming a CSI port is arguable. “The most successful tactic that the U.S. has used to encourage participation in its freight security programs is through the use of economic incentives.” It would logically follow that the motivation for becoming a CSI port stems from the economic incentives of expedited processing rather that the opportunity to station foreign customs officials at U.S. ports. The idea that reciprocity is the primary reason for becoming a CSI port is also drawn into question by the widely held belief by port officials that terrorism is not a major threat to their ports. If foreign ports are not concerned about a risk of terrorism, then why would they care if their personnel are able to be stationed at U.S. ports to ensure adequate security measures are followed? Based on these considerations, the economic benefits of CSI offer more incentive to join the security initiative than reciprocity — even though criticism of CSI typically stems from its perceived lack of reciprocity.

---

168 SUZETTE R. GRILOT ET AL., PROTECTING OUR PORTS: DOMESTIC AND INTERNATIONAL POLITICS OF CONTAINERIZED FREIGHT SECURITY 82 (Ashgate Publ’g Grp. 2010).
170 GRILOT ET AL., supra note 179, at 86.
171 Id. at 85.
172 Id. at 83.
F. C-TPAT Adequately Addresses the Problem of Containers Being Loaded Before Reaching Ports

A final problem with CSI is that shippers load the majority of containers at their own facilities, where neither CBP agents nor foreign port agents can supervise, rather than at the port.¹⁷³ Because these containers are loaded outside the supervision of port authorities, the shipper’s own documentation is relied upon to determine the accuracy of the containers’ contents.¹⁷⁴ The obvious problem with this, as mentioned in Part Two, is that a shipper willing to smuggle goods, people, or weapons will likely be willing to conceal the fact that they are engaging in such smuggling.

One way to address this problem would be to push the boarders out even further and extend CSI to the point of origin rather than the foreign port.¹⁷⁵ The problems with this extension become immediately apparent due to CBP’s existing lack of resources. Extending agents beyond foreign ports to the point of origin where the container is initially loaded will require extraordinary resources. More resources would be required to deploy personnel to every shipper’s facilities. Exponentially more funding would be necessary for screening and scanning equipment to be available at every shipping facility compared with the equipment already in demand at foreign ports. The flow of trade would be further interrupted by an increased number of inspections, causing greater tension between the U.S. and the foreign country.¹⁷⁶

¹⁷⁴ Id.
¹⁷⁶ See Id. n.99
The appropriate resolution to this problem is C-TPAT. C-TPAT is self-policing.\textsuperscript{177} This aspect of C-TPAT lends itself ideally to addressing this problem because continual handholding by the CBP is not necessary. By relying upon C-TPAT certification, DHS can most efficiently address the problem that shippers load the majority of containers at their own facilities outside of port authority supervision. CBP officials continue to monitor C-TPAT members, but certification as a C-TPAT entity means that the shipper has already established that their entire supply chain is secure and they are trustworthy. This is a prime example of how the building blocks of CBP’s layered security strategy comingle in a collective effort to secure containerized cargo from the point of origin to the point of delivery.

G. CBP’s Layered Security Strategy Has Effectively “Pushed the Borders Outward” in the Short-Term and Will Enhance Global Trade in the Long-Term

The U.S. has effectively extended control over inbound containerized cargo beyond its geographic borders.\textsuperscript{178} With CBP agents stationed at CSI ports internationally in positions of oversight, over 10,000 C-TPAT partner entities with more expected in the coming years, and control over entry of cargo which fails to satisfy the 24-Hour Rule, CBP has increased security measures abroad in the short-term using a layered security strategy.

With continued multilateral support and agency development, CBP’s layered security strategy is actually capable of enhancing global trade in the long-term.\textsuperscript{179} This


\textsuperscript{179} Id. at 244–50.
enhancement of free trade along with increased maritime trade security is something which has eluded Doha Round negotiations at the WTO level and stands against the attacks of 9/11. The long-term effects of continued support of CBP’s existing layered security approach are threefold: (1) global harmonization of security measures and reduced transaction costs; (2) disaggregation of borders; and (3) fewer distinctions between domestic and international transactions in goods.\textsuperscript{180}

Global harmonization would result from the adoption of common international security standards, thus increasing inter-jurisdictional transparency and reducing the costs of gathering information and complying with various sets of security measures.\textsuperscript{181} This standardization of maritime security initiatives would simplify compliance by creating a universal standard. Entities interested in expanding trade to additional countries would be able to easily do so because there would be minimal to no additional security measures required by new markets. Transaction costs will additionally decrease as procedures become global and no longer require unique procedures and policies to be negotiated with foreign countries on an individual basis.\textsuperscript{182}

Disaggregation of borders will result from less emphasis being placed on geographic borders in terms of international trade security. The locations of a country’s trade security functions will become far less precisely mirrored by the location of the country’s geographic borders.\textsuperscript{183} CBP agents, in turn, will become more global in nature and less tied to geographic borders. These anomalies culminate to disaggregate and deemphasize the importance of a country’s geographic boundary as far as international

\textsuperscript{180} Id. at 244–47.
\textsuperscript{181} Id. at 244–45.
\textsuperscript{182} Id. at 246.
\textsuperscript{183} Id. at 247.
trade is concerned.

The disaggregation of borders will also eliminate many distinctions between domestic and international transactions in goods.\textsuperscript{184} The same harmonization of global security initiatives that results in lowering international transaction costs may result in increased domestic transaction costs.\textsuperscript{185} As international security measures regarding trade become more standardized, the application of such standards will similarly become more broad. The increased costs to domestic transactions will not be without benefits. The security of domestic goods will increase due to compliance with the additional security measures being implemented at the international level. Some argue this application of international standards at the domestic level is necessary if threats of terrorism are to be seriously addressed — arguing the risk when shipping goods from Texas to Colorado is the same as when shipping goods from Canada to the U.S.\textsuperscript{186} Increasing domestic security standards to mirror the more stringent international security standards would also decrease the security obstacles domestic traders would otherwise face when electing to engage in global trade. Eliminating distinctions between international and domestic trade will result in an increase in the number of participants engaging in international trade.

\textbf{IV. CONCLUSION}

Maritime container security has been reinvented since 9/11. There are multiple ways to approach the issue of container security, each offering its own set of criticism.

\begin{flushleft}
\textsuperscript{184} \textit{Id.}
\textsuperscript{185} \textit{Id.} at 248.
\end{flushleft}
DHS has elected to pursue a layered security strategy developed under CBP and the U.S. Coast Guard. The building blocks of this layered security strategy include CSI, C-TPAT, the 24-Hour Rule, ATS, and the ISPS Code adopted by the IMO at the strong suggestion of the U.S. Coast Guard. This layered security approach certainly has room for improvement, but these agencies and initiatives remain young prospects with great potential for the future of container security.

CSI, along with the other building blocks of CBP’s layered security strategy, should be bolstered to increase trade security in the short-term and enhance global trade in the long-term. SFI’s 100 percent scanning requirement is an unrealistic goal and will not be achieved by the July 12, 2012 deadline. DHS is clearly supporting its risk-based, layered security approach. However, DHS needs to file its formal findings regarding the feasibility, or lack thereof, of SFI so Congress can be informed about the status of DHS’s maritime security stance. Perhaps, if DHS were to do this, legislation similar to the SAFE Port Reauthorization Act of 2011 would gain more substantial traction.

The borders of maritime trade have been pushed outward. The future of CSI should entail expansion and likely capacity-building assistance for developing and least-developed countries. Container security has improved since 9/11, but the threat has far from been eliminated. CBP must receive additional resources to develop technology, procedures, and infrastructure capable of pre-screening 100 percent of cargo to identify containers that are high-risk, inspecting these high-risk containers through more efficient means allowing 100 percent scanning rates of containers that have been flagged as high-risk, more effective scanners capable of detecting threatening nuclear materials, and

---

187 See Bowman, supra note 178, at 243.
smarter containers that allow identification and monitoring of contents and tampering.

Bibliography

Books

R. V. G. CLARKE & GRAEME R. NEWMAN, OUTSMARTING THE TERRORISTS (Greenwood Publ’g Grp. 2006).


JOHN F. FRITTELLI ET AL., PORT AND MARITIME SECURITY: BACKGROUND AND ISSUES (Susan Boriotti et al. eds., 2003).

SUZETTE R. GRILOTT, REBECCA J. CRUISE & VALERIE J. D’ERMAN, PROTECTING OUR PORTS: DOMESTIC AND INTERNATIONAL POLITICS OF CONTAINERIZED FREIGHT SECURITY (Ashgate Publ’g Grp. 2010).

THOMAS PRESTON, FROM LAMBS TO LIONS: FUTURE SECURITY RELATIONSHIPS IN A WORLD OF BIOLOGICAL AND NUCLEAR WEAPONS (2007).

Journal Articles


**Statutes**


**Other Sources**


Rossella Brevetti, *Customs: Rep. Thompson Faults DHS’ Implementation of SAFE Port*


