South Carolina Journal of International Law and Business

Volume 5
Issue 2 *Spring*

Article 5

2009

Ins and Outs of Modern Ports: Rethinking Container Security

Jennifer L. North

THE INS AND OUTS OF MODERN PORTS: RETHINKING CONTAINER SECURITY

*Jennifer L. North**

This paper specifically addresses those measures taken since September 11, 2001, that deal directly with the security of our cargo containers, the largest segment of the international supply chain. Part One provides a backdrop for legislation of trade and port security. Part Two discusses the law mandating various measures for cargo security. Part Three addresses differences between the industry experts and Congress on how best to tackle security issues relating to containers.

The primary focus of this paper deals with the Security and Accountability for Every Port Act of 2006, which stands apart from the Maritime Transportation Security Act of 2002,[1] but remains an integral part of maritime security. The SAFE Port Act[2] brought together several initiatives already in practice, and some other seemingly unrelated legislation.[3] The three initiatives discussed in this paper are the Container Security Initiative,[4] Customs-Trade Partnership Against Terrorism,[5] and the much discussed 100 percent scanning amendment

* Professor of Legal Writing, Charleston School of Law; LL.M., Tulane Law School; J.D., Texas Wesleyan University School of Law. The author wishes to express her appreciation to the University of South Carolina School of Law, and the student editors, in particular Suzanne White, of the South Carolina Journal of International Law & Business, for their invitation to the participate in this symposium, and their generous support throughout the development of this article.

1 Pub. L. No. 107-295, 116 Stat. 2064 (2006).

2 Pub. L. No. 109-347, 120 Stat. 1884 (2006). The Security and Accountability for Every Port Act of 2006 codified several measures relating to port security: Transportation Worker Identity Cards (TWIC); interagency operational center for port security; port security grant program; Container Security Initiative; foreign port assessments; Customs Trade Partnership Against Terrorism; Domestic Nuclear Detection Office; funds for Integrated Deepwater System Program – US Coast Guard modernization program; and implemented regulations for online gambling.

3 The Unlawful Internet Gambling regulation was added at the 11th hour.

4 6 U.S.C. § 945 (2006).

5 6 U.S.C. § 961-73.

to the SAFE Ports Act, found in the Implementing Recommendations of the 9/11 Commission Act of 2007.[6]

I. THE BACKDROP FOR LEGISLATION OF TRADE AND PORT SECURITY

The expanse of global trade is woven into the history and the future of nations. The maritime industry is the primary system in which trade traverses the world, and the container is the means by which 95 percent of all goods travel.[7] Although the shipping container has been utilized for arguably 200 years, it was not until the 1950s when the U.S. Army began using containers to ship supplies that containers started to become the standard for transporting goods in numerous industries.[8] Today, container sizes are standardized to allow for the greatest flexibility in shipping, and ships are special built to carry several thousand containers.

The International Maritime Organization (IMO),[9] a specialized agency of the United Nations, is considered to be the foremost international gatekeeper for maritime law, despite having no sovereign authority. Contracting Parties, however, as signatories to various conventions, are generally required to comply.[10] Failure to comply can

---

[6] Pub. L. No. 110-53, § 1701, 121 Stat. 266, 489 (2007).

[7] *See* Veronique de Rugy, *Is Port Security Spending Making Us Safer?*3 (Am. Enterprise Inst. of Pub. Pol'y Research, Working Paper No.115,(2005).

[8] Container History, (2006), http://www.globalsecurity.rog/military/systems/container-history.htm (last visited April 14, 2009); *See generally* MARC LEVINSON, THE BOX: HOW THE SHIPPING CONTAINER MADE THE WORLD SMALLER AND THE WORLD ECONOMY BIGGER, (2006) (detailing the history of the modern shipping container).

[9] International Maritime Organization, http://www.imo.org (last visited Feb. 24, 2009). Throughout its 61 years of existence, the IMO has promulgated international conventions and protocols covering maritime safety and security, prevention and reduction of pollution, preparedness for and response to maritime accidents and other issues including the facilitation of maritime traffic and salvage. IMO: 50 years, 50 treaties, http://imo.org/Safety/mainframe.asp?topic_id=1709&doc_id=9076 (last visited Feb. 24, 2009).

[10] There are 148 Contracting Parties to SOLAS (International Convention for the Safety of Life at Sea). The International Ship and Port Security Code (ISPS) is an amendment to SOLAS, and as such compliance is mandated. FAQ on ISPS Code and maritime security, http://www.imo.org/Newsroom/mainframe.asp?topic_id=897 (last visited Feb. 25, 2009). In contrast, there are 167 member states in the IMO. IMO: 50 years, 50 treaties,

result in a range of consequences.[11] The IMO was created in response to the Titanic disaster, and through time, it has continued to issue guidelines about those things most concerning the maritime industry, with the main objective to keep commerce flowing.

A timely and recent example of internationally driven and domestically implemented guidelines is the International Ship and Port Facility Security Code (ISPS), which was promulgated in direct response to the terrorist attacks on September 11, 2001.[12] Although the attacks did not come via a maritime pathway, it was clear that in looking at vulnerable entry points, most ports could be a favored target.[13] The ISPS lays out minimum security requirements for ships and ports with the main objectives being to detect security threats and implement security measures; to establish roles and responsibilities for entities involved in maritime security; to collate and promulgate security related information; and to provide a methodology for security assessments that will aid in developing plans and procedures to respond to various security threats.[14]

The extent of maritime trade cannot be underestimated. United States ports move 99.4 percent of overseas trade by volume, and 64.1

---

http://imo.org/Safety/mainframe.asp?topic_id=1709&doc_id=9076 (last visited Feb. 24, 2009).

[11] Possible sanctions are enforced through member state action: "contracting governments should direct those ships flying their flag [which are not in compliance] to immediately discontinue operations until they have been issued the required certificate." FAQ on ISPS Code and maritime security, http://www.imo.org/Newsroom/mainframe.asp?topic_id=897 (last visited Feb. 25, 2009). They may also detain a ship in port that does not have the required certificate, expel the ship, refuse entry to the ship, or curtail the operations of the ship. In sum "[t]he measures which are in place have been designed in such a way to ensure that those ships which do not have certificates find themselves out of the market in the shortest possible time." *Id.* Further, owners may direct their ships not to call at ports that are not in compliance, as the ships may encounter problems at subsequent ports of call. *Id.* This is similar to the idea behind the benefits to being a CSI partner discussed later in this article.

[12] The ISPS is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of 9/11 attacks in the United States. FAQ on ISPS Code and maritime security, http://www.imo.org/ Newsroom/ mainframe.asp?topic_id=897 (last visited Feb. 25, 2009).

[13] *See* de Rugy, *supra* note 7, at 11.

[14] FAQ on ISPS Code, *supra* note 12 ("the whole idea of the ISPS Code is to reduce the vulnerability of the industry to attack thus countering the threat and reducing the risk.")

per cent by value, according to the U.S. Census bureau.[15] This equates to approximately 11 million containers annually that are offloaded in United States ports.[16] Projections vary, but the Department of Transportation estimates that total freight moved through United States Ports will increase by at least 50 percent by the year 2020 (as compared to 2001), and international container traffic will more than double. Currently worldwide container traffic is estimated to be at 100 million containers annually.[17] With the current volume of traffic and the projected numbers, there is no doubt that infrastructure will need additional expansion, and processing technologies will need to continue development, both of which will aid in the efficiency and safety of the maritime industry.[18] The disruption of the supply chain is of paramount concern to the industry. Aside from the threat of terrorism, the industry is also concerned about regional conflicts, natural disasters, organized crime, changes in political administration, funding shifts, and unforeseen technological developments.[19]

Disruptions are costly, with it being estimated that a two day closure of a port would cost $58 billion, while a detonation of a nuclear device could cause up to $1 trillion dollars in damage. There is potential that this type of catastrophe could plunge a nation, or the world, into a dangerous economic downturn.[20]

II. U.S. MARITIME SECURITY LAW

The United States has been a leader in evaluating and implementing port security measures and has passed initial legislation addressing the recognized concerns. The Maritime Transportation and Security Act (MTSA), passed before the ISPS, but paralleling it,

---

[15] U.S. Public Port Facts (July 2008), http://www.aapa-ports.org/files/PDFs/facts.pdf.

[16] Recently CBP Commissioner testified that 32,000 containers arrive daily. *Cargo and Container Security: Before the Subcomm. on Homeland Sec. of the H. Comm. on Appropriations*, 111th Cong. (2009) (statement of Jayson Ahern, Acting Commissioner, U.S. Customs & Border Protection) *available at* http://www.dhs.gov/ynews/testimony/testimony_1238603858 77.shtm..

[17] Container Security Initiative Strategic Plan, http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf.

[18] *Id.*

[19] *Id.*

[20] *See generally* Container Security, "Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors," July 2003, GAO-03-770, U.S. GAO, 8.

requires that security be evaluated at port facilities and on vessels.[21] Once evaluated, vessel owners and port managers are expected to implement plans specific to their responsibilities in order to improve overall security in the maritime industry. Among the interests noted in the MTSA are generally protecting ports and waterways from terrorist attacks. Specifically the Act lists areas for ports to consider an evaluation such as conducting vulnerability assessments, developing security plans and screening procedures for cargo, establishing security patrols and delineating restricted areas, implementing personal identification procedures, access control measures, and installing surveillance equipment where appropriate.[22]

The SAFE Port Act of 2006 overlaps to some extent the directives of the MTSA when it addresses the overall security of the international supply chain.[23] The Act advocates a multi-agency approach to develop and implement security standards in the chain, taking into account proposed and established practices of foreign governments and international organizations.[24] Considerations for developing these programs include describing the roles, responsibilities, and authorities who are part of the security chain and identifying gaps, and unnecessary overlaps that should be eliminated.[25] The Department of Homeland Security (DHS) is instructed to make recommendations regarding legislation and regulations, and potential organizational changes to improve security.[26] Resources available and cost-benefits need to be considered as well as looking for additional voluntary measures that might enhance security.

Recognizing that additional regulations and legislative requirements can be onerous to the small and medium sized companies, Congress makes reference to considering the effect these measures will have on these companies, adding that a process for sharing intelligence and other information is desirable.[27] Finally, when preventative measures fail, ports should have prudent responses and protocols in

---

[21] Pub. L. No. 107-295, 116 Stat. 2064 (2006).

[22] *Id.*

[23] 6 U.S.C. § 941(b)(12). "International Supply Chain" means 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. 6 U.S.C. § 901(10).

[24] 6 U.S.C. § 941(c).

[25] 6 U.S.C. § 941(b)

[26] *Id.*

[27] 6 U.S.C. §941(b)(8)

place to deal with events affecting the supply chain, and to provide for expeditious resumption in the flow of trade.[28]

A. *CONTAINER SECURITY INITIATIVE*

The Container Security Initiative has been in place since January, 2002, just a few short months following September 11, 2001. It was implemented by U.S. Customs and Border Protection, which functions now as part of the Department of Homeland Security.[29] Aside from one notable addition, the entire initiative laid out by CBP was adopted and codified by the SAFE Ports Act.

The SAFE Ports Act, as it relates to container security, provides for various inspections, screening, and scanning measures to be under taken both at U.S. and foreign ports.[30] Through the Automated Targeting System (ATS) all information about cargo is reviewed and given a risk evaluation; if deemed to be high-risk it will be subject to the various inspection procedures.[31] The ATS is able to provide real time data to inspectors at ports who may request additional scrutiny for these high-risk containers. This may include intrusive inspections, where containers are opened and visually inspected, but this is rare.

---

[28] 6 U.S.C. §941(b)(10)

[29] U.S. Custom and Border Protection, Container Security Initiative, http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade_security/csi.xml (last visited Apr. 30, 2009).

[30] 6 U.S.C. § 945. "Examination" means an inspection of cargo to detect the presence of misdeclared, restricted, or prohibited items that utilizes nonintrusive imaging and detection technology. 6 U.S.C. § 901(8). "Inspection" means the comprehensive process used by the CBP to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws; the process may include screening, conducting an examination, or conducting a search. 6 U.S.C. § 901(9). "Scan" means to utilize nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container. 6 U.S.C. § 901(12). "Screen" means a visual or automated review of information about goods, including a manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo. 6 U.S.C. § 901(13). "Search" means an intrusive examination in which a container is opened and its contents are devanned and visually inspected for the presence of misdeclared, restricted, or prohibited items. 6 U.S.C. § 901(14).

[31] 6 U.S.C. § 943.

Usually containers are scanned using x-rays or gamma ray devices that aim to detect dangerous radioactive and nuclear materials.[32]

As is clear, cooperation with foreign governments is essential to ensuring port security. To date, the CBP has been instrumental in partnering with 58 foreign ports to combat known security threats.[33] Through these ports travel 85 percent of the trade entering the United States by vessel. Currently, the CBP is able to "pre-screen" 86 percent of all containers exiting these ports, with a goal to screen 100 percent. The value of the "pre-screening" is that where high-risk factors are indentified, those containers are able to be flagged for further scrutiny.

The Implementing the Recommendations of 9/11 Act of 2007 amended an already controversial feature of the SAFE Ports Act. Under the SAFE Ports Act, Congress mandated 100 percent screening of cargo containers and 100 percent scanning of high-risk containers originating outside the United States.[34] These containers would be screened and scanned (as appropriate) before leaving a U.S. facility.[35] In the SAFE Ports Act, Congress anticipated full implementation of scanning sometime in the future, but the 9/11 Act firmly established July 1, 2012, as the date by which all containers shall be scanned.[36] This provision is one that, coincidentally, was never a goal of CBP when implementing the Container Security Initiative in 2002.[37]

Furthermore, in the 9/11 Act, Congress explicitly stated: "A container that was loaded on a vessel in a foreign port shall not enter

---

[32] 6 U.S.C. § 592.

[33] U.S. Customs and Border Protection, Container Security Fact Sheet (Oct. 2, 2007), http://www.cbp.gov/linkhandler/cgov/trade/cargo_ security/csi/ csi_fact_sheet.ctt/csi_fact_sheet.doc.

[34] 6 U.S.C. § 982.

[35] The SAFE Port Act also created an office for Domestic Nuclear Detection at 6 U.S.C. § 591. Part of the mission of this office would be to scan for radiation all containers entering the United States through the 22 ports which have the greatest volume of entering containers shall be scanned for radiation. 6 U.S.C. § 921(a). By December 31, 2008 this program was mandated to expand to all U.S. ports of entry. 6 U.S.C § 921(h).

[36] 6 U.S.C. 982(b)(2). Full scale implementation was contemplated at the time of the passage of the SAFE Ports Act, but several mitigating factors would allow for a delay in implementation: high false alarm rates; deployment issues at foreign ports; an inability to integrate with existing systems; an overly detrimental impact on the flow of cargo and trade capacity; and an inability to provide automated notification of questionable or high risk cargo as a trigger for further inspection. 6 U.S.C. § 982(b)(4).

[37] 6 U.S.C. 982(b)(2).

the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel."[38]

Other provisions in the SAFE Ports Act followed closely the guidelines the CBP already had in place under the Container Security Initiative. In fact the name CSI transferred into the legislation, where §945 enumerates the actions DHS must take with regard to the movement of containers.[39] Under §945, the Department shall identify and examine or search containers in a foreign port that are bound for the United States.[40] The Department/CBP can accomplish this task by directly inspecting the container or by requesting the host port to conduct the inspection, while CBP observes.[41]

Initially the participating ports were determined via the Secretary through an assessment of "the level of risk for the potential for compromise of containers by terrorists."[42] Other factors considered were the volume of cargo being imported to the United States through the foreign seaport, the results of Coast Guard assessments conducted under 46 U.S.C. § 70108, and the commitment of the foreign government to cooperating with the United States to share critical data, risk management information, and maintaining programs to ensure employee integrity.[43] The Secretary may also consider the potential for validation of security practices at the foreign seaport.[44]

---

[38] Pub. L. No. 110-53, § 1701, 121 Stat. 266, 489 (2007) (amending 6 U.S.C. § 982(b)). Here the deadline to scan can also be delayed if at least two of the following circumstances exist: systems to scan containers are not available for purchase and installation; systems do not have a sufficiently low false alarm rate for use in the supply chain; systems cannot be purchases, deployed, or operated at ports overseas, including if applicable, because a port does not have the physical characteristics to install such a system; systems cannot be integrated, as necessary with existing systems; use of systems that are available to scan containers will significantly impact trade and the flow of cargo; systems do not adequately provide an automated notification of questionable or high risk cargo as a trigger for further inspection by appropriately trained personnel. *Id.*

[39] 6 U.S.C. § 945.

[40] *Id.*

[41] *Id.*

[42] 6 U.S.C. § 945(b)(1).

[43] 6 U.S.C. § 945(b)(2-4)

[44] 6 U.S.C. § 945(b)(5).

When foreign ports sign on to be partners in CSI, they must meet certain requirements. The partnership is truly mutual in that the counterparts of the CBP are invited to station their own customs agents in United States ports to observe inspections/scanning procedures.[45] For overseas inspections, the CBP establishes procedures for the use of nonintrusive nuclear and radiological detective systems. The cost of this equipment, though expensive, is expected to be borne by the foreign host. CBP/CSI teams also continually monitor the inspection techniques, procedures, and technologies used at foreign ports to ensure these ports are in compliance with their CSI partnership agreement.[46] The Secretary of Homeland Security must consult with the Secretary of Energy in establishing the technical capability criteria and the standard operating procedures that pertain to the detection of radiation in order to promote consistency at foreign ports.[47]

The Secretary is authorized to issue "do not load" orders, via existing authorities, in order to prevent the loading of high-risk cargo.[48] The designation of "high-risk" may be reassessed when a scan of the cargo with nonintrusive imaging equipment and radiation detection produces no anomalies, if there has been a satisfactory search of the cargo, or if new information has been received to show that the cargo is safe.[49]

B. *CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM*

The Customs-Trade Partnership Against Terrorism (C-TPAT) is the second initiative complementing CSI that was codified under SAFE Ports Act.[50] The initiative, also begun in 2002, expands the idea of "moving back the borders" even beyond that of what CSI does. In C-TPAT, importers, brokers, forwarders, air, sea, land carriers, contract logistics providers, and other entities in the international supply chain voluntarily enter into partnership with the DHS where they agree to provide additional information regarding the contents of their shipments.[51] While CSI is primarily concerned with the riskiness of the cargo, C-TPAT has a dual purpose to both obtain more information regarding the shipment so risk evaluations can be made, and also to keep the supply chain running as efficiently as possible. When eligible

---

[45] *See* Container Security Initiative Fact Sheet, *supra* note 33.
[46] 6 U.S.C. § 945(e)(1)(c).
[47] 6 U.S.C. § 945(e)(1)(d).
[48] 6 U.S.C. § 945(k)(1).
[49] 6 U.S.C. § 945(k)(1)(a-c).
[50] 6 U.S.C. § 961-973.
[51] 6 U.S.C. § 962.

entities partner under C-TPAT, they receive benefits by meeting or exceeding the program requirements.[52] The participants receive Tier 1, 2, or 3 status, and the various benefits that go along with that designation.[53]

In order to receive any beneficial status designation all entities must meet minimum requirements.[54] The applicants must demonstrate that they have a history of moving cargo in the international supply chain.[55] They further have to show an assessment of its supply chain by reviewing its own business partner requirements, container security, physical security and access controls, personnel security, procedural security, security training and threat awareness, and information technology security.[56] Finally, if determined as necessary by CBP, the entity must implement and maintain additional security measures meeting the criteria of the DHS.[57]

Once the minimum requirements have been met, entities may apply for validation in three phases. Tier 1 status will include a background investigation and extensive documentation review by CBP.[58] The benefits to the Tier 1 status allow a reduction in the risk score assigned by ATS.[59] Tier 2 status involves those satisfactory Tier 1 participants whose security practices are assessed onsite by the Department.[60] This assessment conducted at foreign locations should be completed within one year of Tier 1 validation.[61] Tier 2 benefits include reduced risk scores in ATS, reduced examinations of cargo, and priority searches of cargo.[62] Tier 3 participants receive additional benefits beyond Tier 2 status.[63] Tier 3 participants are those who have demonstrated a sustained commitment to maintaining satisfactory security measures exceeding those of the Tier 2 entity. Tier 3 status is granted when participants are in compliance with any additional

---

52 6 U.S.C. § 961(a) (DHS "is authorized to establish a voluntary government private sector program . . . to strengthen and improve the overall security . . . and to facilitate the movement of secure cargo . . . by providing benefits to participants meeting or exceeding the program requirements").

53 6 U.S.C. §§ 964-966.

54 6 U.S.C. § 963.

55 6 U.S.C. § 963(1)

56 6 U.S.C. § 963(2)(A-G)

57 6 U.S.C. § 963(3-4)

58 6 U.S.C. § 964(b)

59 6 U.S.C. § 964(a).

60 6 U.S.C. § 965.

61 6 U.S.C. § 965(a).

62 6 U.S.C. § 965(b).

63 6 U.S.C. § 966.

guidelines set out by the Secretary, to include submission of additional information regarding cargo prior to loading, and utilization of container security devices, technologies, policies and practices that meet the DHS standards and criteria for security.[64] Incentives to become Tier 3 participants include expedited release of a cargo in destination ports within the US 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.[65]

All C-TPAT participants are subject to reevaluation and will suffer consequences if found not be in compliance.[66] An example of noncompliance that will suspend or expel a participant is providing false or misleading information during the validation process.[67] CBP is authorized to publish the names of those suspended or expelled entities in the Federal Register, and participants may appeal adverse decisions within 90 days.[68] Each participant shall be revalidated not less than every four years[69] and importers of non-containerized cargoes are also eligible to participate in C-TPAT.[70]

A similar benefit of priority is bestowed on vessels that have certain other certifications under the SAFE Act. During a maritime security incident vessels with an approved security plan or valid international ship security certificate, and manned by approved individuals in accordance with 46 U.S.C. §70105(b)(2)(B) and that is operated by validated participants in C-TPAT will get priority for inspection and clearance of its cargo.[71]

Cargo may also be given priority where it is entering a port directly from a foreign seaport designated under the CSI, is from the supply chain of a validated C-TPAT participant, or if it has undergone a nuclear, radiological detection scan, an x-ray density, or other imaging scan, and a system to positively identify the container at the last port of departure prior to arrival in the US, and that data has been evaluated and analyzed by CBP.[72]

---

[64] 6 U.S.C. § 966(b)
[65] 6 U.S.C. § 966(c).
[66] 6 U.S.C. § 967.
[67] 6 U.S.C. § 967(b).
[68] 6 U.S.C. § 967(c).
[69] 6 U.S.C. § 969.
[70] 6 U.S.C. § 970.
[71] 6 U.S.C. § 942(b).
[72] 6 U.S.C. § 942(c).

III. SUPPORTERS AND DETRACTORS

Despite the devastation that could be caused by the explosion of a nuclear device, the 100 percent scanning provision has been controversial for several reasons. When one considers the amount of individual containers that must be scanned prior to leaving a foreign port, the task is enormous, and near impossible.[73] Further, when evaluating the mandate under a cost benefit analysis, experts note that, though catastrophic, the actual risk of this scenario is quite low--so low that the amount expended on this program exceeds the benefit received. A third factor that is sometimes noted is that the actual scanning equipment is not reliable where nuclear material has been shielded, and the machines can produce numerous false positive results.

The Government Accounting Office (GAO) has conducted nonpartisan reviews of the International Supply Chain and the Container Security Initiative, and noted both positive and negative aspects.[74] The leaders of CBP and the Domestic Nuclear Detection Office (DNDO) recently testified before Congress reporting on whether goals laid out in the SAFE Ports Act and the 9/11 Act have been met.[75] Department officials are generally upbeat about the progress that has been made in developing international partnerships and being viewed as the leader in the world for supply chain security.[76] The underlying approach heralded by CBP is a risk management model.[77]

CBP is collecting more, and improved, advance information on cargo, which has allowed for better risk assessments via the ATS before cargo arrives in the United States.[78] Continuing with the multi-

---

[73] This also implicates huge cost and personnel requirements.

[74] *See generally* GAO, *Maritime Security: The SAFE Ports Act: Status and Implementation One Year Later*, GAO-08-126T (2007); GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed*, GAO-08-187 (2008).

[75] *Cargo and Container Security: Hearing before the Subcomm. on Homeland Security of the House Committee on Appropriations*, 111th Cong. (2009) (statement of Jayson Ahern, Acting Commissioner, U.S. Customs & Border Protection), *available at* http://www.dhs.gov/ynews/testimony/testimony_123860385877.shtm .

[76] *Id.*

[77] *Id.* Risk management as used here indicates that choices must be made under both cost benefit ideas as well as keeping in mind the feeling that no gap can be left in the entire system, a potentially impossible task.

[78] *Id.* The CBP Importer Security Filing (also known as 10+2) includes manufacturer (or supplier) name and address, seller (or owner) name and

layered approach favored by the Department, the C-TPAT program has allowed the United States to leverage security where CBP has limited regulatory power.[79] Additionally, C-TPAT continues to be a strong incentive for companies: CBP projects that 3,200 validations will be requested during fiscal year 2009 for both certification and revalidations.[80]

Further, CBP reports that it is able to review 100 percent of all manifests under the CSI program.[81] CBP has partnered with 32 countries and has a presence at 58 ports world-wide. Through these ports, 86 percent of all containerized cargo passes to the United States.[82] Ninety-five percent of examinations requested were performed by the host countries amounting to 74,000 examinations.[83]

CBP is less enthusiastic about the Secure Freight Initiative, specifically in regard to the 100% scanning requirement.[84] While there are pilot projects in place to measure the effectiveness of the program, the CBP admitted that attempting to scan 11.3 million containers presents "significant, operational, technical, and diplomatic

---

address, buyer (or owner) name and address, ship to name and address, container stuffing location, consolidator (Stuffer) name and address, importer or record number/foreign trade zone applicant identification number, consignee number(s), country of origin, and Commodity Harmonized Tariff Schedule of the United States number. In addition, two more data elements are provided by the carriers: the Vessel Stow Plan and Container Status Messaging. *Id.*

[79] Asking for stricter compliance encourages companies to provide additional information, where the United States has no power to legislate this compliance outside the United States..

[80] Ahern, *supra* note 75.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] The Secure Freight Initiative is laid out in the SAFE Ports Act at 6 U.S.C. § 981 and § 981(a) (DHS shall designate three foreign seaports for the establishment of pilot integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment, and ports should be distinct with unique features and differing levels of trade volume). The pilot system will: scan all containers destined for the U.S. that are loaded in such ports; electronically transmit the images and information to US personnel for evaluation and analysis; resolve every radiation alarm according to established Department procedures; utilize the information to enhance the ATS; store the information for later retrieval and analysis; and may provide automated notification of questionable or high risk cargo as a trigger for further inspection by appropriately trained personnel.

challenges."[85] The Commissioner asserted that limited scanning is possible but is currently limited to gate traffic as there is no technology available that would allow scanning in transshipped containers.[86] This scanning is in addition to the scanning that is done for all arriving sea containers prior to release at domestic ports. In the United States, scanning equipment is available at 87 seaports for a total of 409 Radiation Portal Monitors (RPMs). Approximately 98% of all arriving sea-borne containers pass through these entry points. Eighty-three more RPMs will be deployed by the end of fiscal year 2009.[87]

Not to neglect additional security measures, the Commissioner addressed the SAFE Ports Act reference to container security standards and devices,[88] indicating that the procurement of such devices had not yet been successful.

The Commissioner's recent testimony is supported by that of the Acting Director of the Domestic Nuclear Detection Office (DNDO), the agency tasked with reducing the risk of radiological and nuclear

---

[85] Ahern, *supra* note 75. Challenges listed include sustainability of the scanning equipment in extreme weather conditions and certain port environments; varying and significant costs of transferring the data back to the United States in real-time; re-configuring port layouts to accommodate the equipment without affecting port efficiency and getting permission of host governments; developing local response protocols for adjudicating alarms; addressing health and safety concerns of host governments and local trucking and labor unions; identifying who will incur the costs for operating and maintaining scanning equipment; acquiring necessary trade data prior to processing containers through the SFI system; addressing privacy concerns in regards to scanning the data; concluding agreements with partnering nations and terminal operators to document roles and responsibilities regarding issues such as ownership, operation, and maintenance of the equipment, sharing of information, and import duty and tax considerations; staffing implications of both the foreign customs service and terminal operator; licensing requirements for the scanning technology; host government support for continuing to scan 100 percent of U.S. bound containers after the pilot ends; and potential requirements for reciprocal scanning of U.S. exports.

[86] *Id.*

[87] *Id.* These measures are significant, if not all encompassing, but Ahern describes the risk of using a maritime transportation system to deliver nuclear or radiological device as still low. Many agree that due to handoffs, delays, mixups, and other uncertainties throughout the supply chain, terrorists would be reluctant to transport what would likely be their one and only weapon through an unpredictable system. US Congress shifts away from 100 percent container screening, http://www.shippingonline.cn/info/msg.asp?id+8894.

[88] Ahern, *supra* note 75.

terrorism.[89] The Director noted that impeding the flow of legitimate trade was a consideration as to how RN detection is implemented.[90] The technology currently being used can detect radiation, but there are still problems because the monitors "cannot distinguish between threat materials and naturally occurring radioactive material (NORM), such as kitty litter and ceramic tile."[91] He assured that work is being done to improve detection technology, as well as to reduce false alarms, including testing of a new portal system known as the Advanced Spectroscopic Portal (ASP).[92] He also asserted that these monitors would be able to make intelligent determinations of threatening and non-threatening materials, but ASP would still be unable to detect shielded nuclear materials placed in cargo containers.[93] However, the Cargo Advanced Automated Radiography System (CAARS) is currently in development to address the problem of detecting shielded nuclear material.[94]

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. When the legislation was passed, Democrat leaders attempted to dispel myths about the program that had been hindering its approval and primarily blamed the obstacles on partisan interests.[95] The structure, however, of the legislation indicates that even the Republican majority was cognizant of the potential problem with 100% implementation, as evidenced by the inclusion of several means by

---

[89] *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) *available at* http://www.dhs.gov/ynews/testimony/testimony_1238610092655. The DNDO was created under the SAFE Ports Act. 6 U.S.C. § 591 (establishing an office to coordinate efforts to detect and protect against unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against attack using such devices or materials against the people, territory, or interests of the United States).

[90] *Id.*

[91] *Id.* These detectors are polyvinyl toluene (PVT)-based radiation portal monitors.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] Press Release, Representative Jerrold Nadler, Myths and Realities of 100-Percent Screening (May 3, 2006), http://www/house.gov/list/press/ny08_nadler/MythRealitiesScan050306.html.

which DHS could extend the deadlines of full implementation.[96] Test programs have been in place for nearly two years now, and unfortunately, although successful on a limited scale,[97] it appears that full implementation is too burdensome without an associated improvement in detection capabilities.

While some want to back away from the requirements, Stephen Flynn of the Council on Foreign Relations argues that not enough funds have been appropriated to adequately tackle the issue and that DHS has overstated its accomplishments with regard to the efforts on cargo security.[98] A proponent of "pushing the borders out," Flynn advocates establishing controls at the point of origin of goods, rather than using the port as a starting place for inspection, because the CSI alone cannot fully accomplish its mission.[99] But unlike Congress, Flynn is very critical of assuming radiation monitors can be the last line of defense.[100] Nuclear materials are shielded by design;[101] therefore reliance on monitors that cannot detect shielded material gives a false sense of security. This results in less attention being paid to those containers that do in fact warrant greater scrutiny.[102] Flynn criticizes the honor system used to extract data regarding the content of containers, but in the end

---

[96] 6 U.S.C. § 982.

[97] Ahern, *supra* note 75.

[98] *Overcoming the Flaws in the U.S. Government Efforts to Improve Container, Cargo, and Supply Chain Security: Hearing on Container, Cargo, and Supply Chain Security – Challenges and Opportunities, Before the Subcomm on Homeland Security of the H. Comm. on Appropriations*, 111th Cong. (2008) (statement of Stephen E. Flynn, Jeane J. Kirkpatrick Senior Fellow in National Security Studies, Council on Foreign Relations), *available at* http://opim.wharton.upenn.edu/risk/library/2008-04-02_Flynn_Improving ContainerSecurity.pdf.

[99] *Id.* at 6 (stating that limitations on CSI include a hesitation to overburden the host country with requests to inspect, flaws with the targeting system for high risk containers result in useless inspections, and this strains support for CSI in the host country; the other main concern is that the flow of trade will be interrupted, further causing tension between the U.S. and the host port).

[100] *Id.* at 7.

[101] *Id.*

[102] *See* Jena Baker McNeil, *100 Percent Cargo Container Scanning: A Global Disaster* (2008), *available at* http://www.heritage.org/Research /Homelandsecurity/wm2047.cfm ("the more cargo scanned, the less attention given to each piece of cargo").

concludes that "global networks rely on trust to operate."[103] He asserts that trust will be sustained when the technologies exist to verify detection of dangerous materials.

The IMO agrees with Flynn in that security measures must be implemented prior to departure, at the place where the containers are stuffed.[104] This requires further cooperative efforts from foreign countries and incentives for these nations to buy-in to legislating these new measures. This could be accomplished by contracting with "regulated agents" that maintain satisfactory security measures and by providing C-TPAT-like benefits to those companies who utilize such agents.[105] Inspection of high risk cargo would still be done by control authorities who are best able to dedicate adequate resources to detecting dangerous contents.[106]

Maritime and security trade organizations echo these concerns, as do policy research organizations.[107] But these groups tend to place more weight on a risk-management model and were recently pleased to see that new DHS Secretary Janet Napolitano has a realistic view that full scale implementation of 100% scanning is not possible by 2012.[108] This recent testimony followed several studies and reviews of the

---

[103] Flynn, *supra* note 98 (the objective is to continue development of the technologies that will enable detection of nuclear materials, but urge the government to provide incentives for private industry to develop these tools).

[104] Chris Trelawny, *Containerised Cargo Security – a Case for "Joined Up" Government*, IMO News, June 7, 2006, at 12.

[105] *Id.* (cargo could be fast tracked – this is thought to provide enough incentive for shippers to comply).

[106] *Id.*

[107] *See generally* Henry H. Willis & David S. Ortiz, the Rand Corp., EVALUATING THE SECURITY OF THE GLOBAL CONTAINERIZED SUPPLY CHAIN (2004), http://www.rand.org/pubs/technical_reports/2004/Rand_TR214.pdf; Veronique de Rugy, *Is Port Security Spending Making Us Safer?* (Am. Enterprise Inst. of Pub. Pol'y Res., Working Paper No.115, 2005); James Jay Carafano, Ph.D., & Martin Edward Anderson, the Heritage Foundation*Trade Security at Sea: Setting National Priorities for Safeguarding America's Economic Lifeline* (2006), http://www/heritage.org/research/national secuirty /bg1930.cfm; Jim Giermaski, *A Different Theory for 100 Percent Container Scanning* (2007), http://www/securityinfowatch.com/ root+level/1287428; Joseph Straw, *Outlook for Container Scanning* (2008), http://www. securitymanagement.com/print/4692.

[108] *U.S. to Miss 2012 Nuke Screening Deadline*, Feb. 25, 2009. http://www.cbsnews.com/stories/2009/02/25/politics/100days/domesticissues/ main4828501.html.

scanning process that found many problems with the system and blamed DHS of making excuses.[109]

Policy think tanks have said that 100 percent scanning, despite adding no additional security, could even worsen the economy and weaken the supply chain.[110] Requiring scanning of low risk cargo does not add more security to the process and in fact may alienate some trade partners.[111]

There is some indication that Congress is taking notice and may shift its attitude on the 100 percent scan mandate. At the same House Appropriations Homeland Security Subcommittee last week where the leaders of CBP and DNDO testified, several law makers expressed concerns that the challenges and expense of implementing such a regime outweighs any gains.[112]

IV. CONCLUSION

Regardless of the debated effectiveness of the legislation, legislators need to keep the true objective in mind, and that is the safety and security of the nation. There are enough voices on either side of the argument that the issue of 100 percent scanning deserves further inquiry. If it is true that scanning cannot adequately protect against the entry of radioactive materials in all forms, then Congress must give way and do the hard work of developing measures as close to fail-safe as possible. That likely means deemphasizing scanning and finding alternative detection methods that fit into the multi-layered system of protection that now surrounds America.

---

[109] Matthew Rusling, *Study Blasts Container Scanning Process*, March 2009, http://www.nationaldefensemagazine.org/archive/2009/March/Pages/ Study Blasts ContainerScanningProcess.aspx (The study cited was "Measuring the Operational Impact of Container Inspections at International Ports" by Nitin Bakshi, Stephen E. Flynn, and Noah Gans.).

[110] Jena Baker McNeil, *Disaster of 100 Percent Maritime Cargo Scanning Not Lost on Napolitano*, The Heritage Foundation (2009), *available at* http://www.heritage.org/Research/HomelandSecuirty/wm2288.cfm. *See also* McNeil, *supra* note 102.

[111] *Id.* (noting that some Asian and European countries have indicated it would be a barrier to trade). *See also U.S. to Miss 2012 Nuke Screening Deadline, supra* note 108. (noting that at least 27 countries and major industrial associations have raised significant concerns about the effect of the law).

[112] *US Congress Shifts Away From 100pc Container Screening*, Apr. 8, 2009, http://shippingonline.cn/info/msg.asp?id=8894.