A Report on Port & Maritime Security

An Agenda to Enhance America's Security

Congressional
Port Security Caucus

June 2007

Executive Summary

Almost two billion tons of cargo in 21 million containers travel through America's ports annually. This amounts to nearly $800 billion dollars worth of domestic and international freight.

Each container is an element of world economic vitality, yet a potential weapon of mass destruction in the hands of a terrorist. As Members of Congress who represent America's ports, we work everyday to ensure their continued success. At the same time, we feel strongly that our nation has not given maritime security the same attention or focus which has been devoted to air transport security since 9/11.

There have been some notable enhancements to port security, including the Maritime Transportation Safety Act (MTSA) of 2002. MTSA required, among other things, the establishment of groups coined Area Maritime Security Committees in all the nation's ports to coordinate the activities of all port stakeholders, including other federal, local and state agencies, industry and the boating public.

Most recently is the approval by Congress and signing into law the SAFE Port/ Greenlane bill on October 13, 2006. The SAFE Port Act authorizes $3.4 billion annually over five years for port security and $400 million a year over five years for risk-based grants for training and exercises at ports. It requires the nation's 22 largest ports, which handle 98 percent of all cargo coming into the U.S. to scan all containers through the use of radiation detectors by the end of 2007. The Department of Homeland Security (DHS) will be required to establish pilot programs at three foreign ports to test technology for nonintrusive cargo inspections. Additionally, the law establishes new benefits for trusted shippers such as fewer customs inspections – generally known as Greenlane benefits.

In the 110th Congress H.R. 1, which implemented the 9/11 Commission Recommendations passed the House of Representatives by a wide margin. Although, there were no 9/11 Recommendations directing maritime security, as there were for aviation, the Commission acknowledged that the opportunity to do harm is as great in the maritime arena as in the air. H.R. 1 moved forward mandating that all containers bound for the United States will be scanned in the next 3-5 years as well as seals be placed on containers after they are scanned and secured.

The SAFE Port/Greenlanes law and the passage of H.R. 1 is a large step in the right direction to securing the global supply chain, however, these measures do not address all of our maritime security problems and leave unanswered questions. There is still more work to be done. This report will focus on three primary areas of improvement. First, going forward, we need to improve technology. We need to provide incentives to accelerate the design and implementation of technology to reach the ultimate goal of 100% container screening, tamper proof and secure port worker identity cards, and better detection of biological, chemical and nuclear threats.

Second, we must enhance the processes for scanning at the port of embarkation and advance intelligence analysis to project, anticipate and stop terrorist attacks before they happen. Our goal should be to prevent any weapons or harmful materials from ever making it to the shores of the United States. We must detect, intercept and disarm any threat at the port where it originates. Maritime security is an international issue. All nations must cooperate and shippers must be held responsible for verifying the contents of any container. Someone must be held responsible and accountable for the contents throughout the entire shipment.

Third, we must strengthen international cooperation, as commerce moves through international channels, and inside America's ports through coordination, collaboration, and communication. Accountability and responsibility should be spread across multiple agencies and players.

America is spending substantially more to keep our airports, roadways, and government buildings secure; yet, it is hard to imagine a more grave threat to our homeland security than a nuclear weapon smuggled into one of America's major port cities.

We hope that through these recommendations our government, business and industry can continue to work together to determine the right solutions and the right balance to secure our ports and keep commerce moving.

As co-chairs of the Congressional Port Security Caucus, we put forth the following recommendations to improve security in our nation's ports.

Summary of Recommendations

- The President should put a senior officer in government in charge of Port and Global Supply Chain Security.
- The DNI and the Secretary of Homeland Security should create a senior level executive in each agency to oversee and coordinate port and global supply chain security intelligence.
- The DNI should establish a program to watch over Port Security intelligence and to train analysts to understand this threat.
- The DNI should enhance intelligence sharing with local law enforcement and should include and work with private port industry security and port employees to bring in all available intelligence.
- The DNI should establish systems and protocols to address port and global supply chain security intelligence with our trading partners.
- Congress should direct and fully fund an expedited build-out of Project Seahawk and JHOC's at all U.S. ports.
- Congress should appoint a task force of government, industry, transportation services to establish a process to determine protocols to get a port up and running after an incident.
- All Federal Departments and Agencies should redouble their efforts at sharing technology and expertise so that we can move port security technology forward and into as many domestic and foreign ports as possible.
- DHS should speed the development of a TWIC program, including a system of wireless readers in our ports.
- DHS should implement TWIC cards but we strongly encourage that privacy standards be established to ensure the sensitive and personally identifiable information be kept secure with appropriate access by law enforcement.
- The President should direct an assessment of all strategic ports world-wide, and complete a timeline of implementing port security screening technology.

Representative C.A. Dutch Ruppersberger
Co-Chair Port Security Caucus

Representative Henry Brown
Co-Chair Port Security Caucus

Section I

Port Security -- America at Risk

On August 16, 2006, Terminal 18 on Harbor Island, within the Port of Seattle, was evacuated and shut down for nearly 5 hours. A 500-yard safety zone on land surrounding the terminal was created, as well as a 300-yard safety zone along the Seattle waterfront. Bomb-sniffing dogs had reacted when performing routine monitoring of incoming cargo containers. The containers were from Pakistan and were loaded onto a vessel originating in Hong Kong. Thankfully, no bombs or explosives were found in the containers, and all tests for radioactive material came back negative.

What happens when the headline reads: **"Nuke found at Port"**? America needs to be better prepared to prevent such a potentially catastrophic event. The events of 9/11 changed everything. Port security, however, has not received the same emphasis nor resources invested in air transportation security. Unlike our air transport system, when it comes to port security there is no central government authority in charge. Responsibility and accountability are spread among a diverse array of federal, state, and local law enforcement and military agencies, and there is a high expectation, due to the large geographic and diverse nature of ports and individual facilities that the private sector should be trusted to police itself.

At foreign ports and on the high seas, the lead agencies are Customs and Border Patrol and the U.S. Navy. In many cases, as ships enter U.S. waters, the Coast Guard assumes a greater responsibility. U.S. ports themselves are a diverse mixture of private/public entities managed by state governments or multi-state public entities which contract with private companies to provide port management. Roads and traffic into the port are protected by local police agencies with little training, equipment or expertise in assessing international terrorist threats.

Imagine a future Assistant to the President for National Security waking the President in the middle of the night to report that Naval Intelligence has just confirmed that a cargo container on board a foreign-flagged vessel was emitting radioactivity in high concentrations and is suspected of being a terrorist threat. Before the President could take decisive action to prevent an attack on the United States, he would first have to ask the question: "Where is the ship?" The answer is essential in order to know whether to direct the Pentagon or the

Coast Guard or the FBI or the CIA, or even a local governor to take immediate action. The location of the ship, not the efficacy of the response, would decide which officer of our government was in charge of protecting the homeland.

Safety vs. Commerce

It is critical to find the right balance between increasing port security to desired levels while at the same time not unduly impeding the legitimate flow of commerce and travel.

America's 361 sea and in-land ports handle over 95% of U.S. overseas trade accounting for more that 27% of the Gross Domestic Product. Almost two billion tons of cargo (21 million containers) travel through America's ports annually. This amounts to nearly $800 billion dollars worth of domestic and international freight.[1] Serving consumer demand for international goods and transporting passengers is an essential component of our national economy.

Ninety percent of the world's trade occurs via container cargo shipped in and out of seaports. It is important to the security of the United States and the rest of the world that cargo shipped through seaports is screened for hazardous materials which could be used to make a "dirty bomb", or even worse, a nuclear weapon

Getting port and global supply chain security right will require a partnership between government and the private sector. The federal responsibility should include setting national priorities; minimizing the cost on industry to comply with government regulation; improving information sharing between the public and private sector; and creating incentives to encourage industry to innovate and modernize security technology.

The private sector must do more to work together – shippers, handlers, port facilities managers, and security companies – to integrate and share the burden of security. We need to move closer to the model in air transportation where the airline industry works more hand-in-hand with government regulators. The maritime industry must assume a greater responsibility to understand the terror threat and lead the way on technological innovation.

In the tragic circumstance that we fail to prevent an attack, and something does occur to shut down one of America's ports, who decides when it is safe to open again? If the choice was left to those in charge of protecting our

[1] Port Security Council. Port Security is our National and Economic Security Fact Sheet. (Washington, D.C. : GPO, 2006).

homeland, the port may never re-open. If the decision was left in the hands of industry, market decisions might trump the guarantee that the port is as safe as it can be. It is in the best interest of every American to have both safe and expeditiously flowing commerce.

Possibility and Probability

The top 50 ports in the United States account for about 90% of all cargo tonnage and only 25 U.S. ports account for 98% of all container shipments.[2] The Administration's National Strategy for Maritime Security states that *"the infrastructure and systems that span the maritime domain ... have increasingly become both targets of and potential conveyances for dangerous and illicit activities."*[3]

Since 2000, there have been widely reported instances of terrorist activity against the United States and its allies in the global maritime domain. These activities include, for example, the bombings of the U.S.S. *Cole* and the oil tanker *Limburg* off the Yemeni coast in 2000 and 2002, respectively.[4] Also in 2002, Moroccan authorities foiled an Al-Qaeda plot to attack U.S. and British warships, and possibly commercial vessels, in the Straits of Gibraltar.[5] In the United States, the Department of Homeland Security (DHS) has reported that in early 2001 there was "some suspicion of possible associations between stowaways on Algerian flagged LNG tankers arriving in Boston and persons connected with the so-called 'Millennium Plot'" to bomb targets in the United States.

Maritime and terrorism experts disagree on the likelihood that terrorists will attack or exploit maritime targets. Some experts suggest that such an attack is almost inevitable, given their own information and beliefs about terrorist activities. For example, according to press reports, a senior U.S. military officer has asserted that "it's just a matter of time until the terrorists try to use a maritime attack against us."[6] Similarly, Lloyd's of London, a global insurance company, reportedly considers an attack on a cruise ship "a high likelihood."[7] According to another press report, the operations and emergency management

---

[2] U.S. Congress, House of Representatives, Maritime Transportation Security Act of 2002 conference Report, H.Rept. 107-777, p. 4.

[3] U.S. Dept. of Homeland Security (DHS) and U.S. Dept. of Defense (DOD). *The National Strategy for Maritime Security*. Sept. 2005. p2.

[4] Ships as Terrorist Targets." *American Shipper*. November, 2002. p. 59.

[5] Sawer, P. "Terror Plot to Blow Up Navy Warships is Foiled." *The Evening Standard*. London. June 11, 2002. p. 4.

[6] Gen. R. Eberhart, U.S. Northern Command, as quoted in "Militants Eyeing Seaborne Attack, U.S. General Says." Reuters. Aug. 25, 2004.

[7] Stanley, B. "Seaports Eye Terror Threat." Associated Press. Jan. 5, 2004.

director for the Port of Los Angeles has stated that the probability of a nuclear attack at his port is not low, and that measures to prevent such an attack are the ports' top priority.[8]

Analysis of the likelihood of a maritime terrorist attack must take into account the nature of the attack in question. One analyst believes that there is a "low probability" terrorists would try to use a large ship, such as an oil tanker or cargo ship, as a weapon because of the complexity of doing so; however attacks by small boats are more likely because they "satisfy the overwhelming terrorist requirement for simplicity."[9] Critical to remember, however, is placing nuclear components in a cargo container is not terribly complex.

The key challenge in determining the likelihood of a terrorist attack on a U.S. port is reducing uncertainty. Historic terrorist activity is not necessarily a reliable predictor of future activity, so scenarios derived from attacks like that on the U.S.S. *Cole* may not help prepare for actual future attacks. Furthermore, information about the ongoing motivations, capabilities, and plans of terrorist groups is limited and typically not in the public domain. As the President's National Strategy for Homeland Security stated in 2002, *"the ambiguous nature of most intelligence on terrorist threats means that ... decisions must often be made in conditions of great uncertainty."*[10] Terrorist intelligence gathered by U.S. and foreign agencies may reduce this uncertainty, but is unlikely to eliminate it.

[8] Gorman, S. and S.J. Freedberg, Jr. "Early Warning." *The National Journal.* June 11, 2005.
[9] Murphy, M. Feb. 1, 2006.
[10] U.S. Office of Homeland Security. *National Strategy for Homeland Security.* July 16, 2002.

Section II

Some Progress Since 9/11

The Department of Homeland Security (DHS) was created in response to the terror attacks of 9/11 to bring disparate agencies and organizations together to assist with the collaboration of data and intelligence and the efficient application of government assets against a terrorist threat. The agency itself has experienced a mixed record of success in achieving these goals.

In regards to U.S. port security, there are four primary players: the U.S. Customs and Border Protection (CBP), United States Coast Guard (USCG), the local port authority, and the private contractor who functions as the port terminal operator.

CBP, through a variety of means, screens cargo manifests and some cargo before it is loaded onto a foreign ship bound for the U.S. CBP is in the business of preventing terrorists and terrorist weapons from entering the United States by eliminating potential threats before they arrive at our borders and ports. [11] They currently utilize large-scale x-ray and gamma ray machines and radiation detection devices to screen cargo.

Within the MTSA there are layered plans for maritime security. At each level; National, local, terminal and vessel, security plans are created. USCG regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance with the comprehensive security plan. While the USCG governs and polices the navigable waterways of the U.S., the Port authority maintains the physical infrastructure and often provides additional security for their facility. Terminal operators are generally responsible for the area within the facility that serves as a loading, unloading, or transfer point for the cargo.

Presently, CBP operates in conjunction with the other players, over 680 radiation portal monitors at our nation's ports of entry, and utilizes over 170 large scale non-intrusive devices to examine cargo. Over 600 canine detection teams, which are capable of identifying narcotics, billed currency, human

[11] Department of Homeland Security. Who Secures the Ports, 2006 (Washington, D.C. : GPO, 2006) 1.

beings, explosives, agricultural pests, and chemical weapons, are also deployed at our ports of entry.[12]

Early Initiatives at Collaboration

The most advanced collaborative effort on port security is Project Seahawk in Charleston, South Carolina. It is a project created to bring together federal, state, and local entities – essentially everyone with a role is securing the Port of Charleston – putting them in one room and making them work together. Coordination and information sharing between these diverse agencies builds in layers of security, making the net ever more effective

Project Seahawk was created as a federal pilot project in March 2003, specifically for Charleston, S.C. to enhance the protection, security, and infrastructure of seaports nationally. It is administered by the U.S. Attorney's Office for the District of South Carolina and is focused on the Port of Charleston, South Carolina. The project includes 47 agencies that can be called upon on an as-needed, part-time, or full-time basis. At the federal level, in addition to the U.S. Attorney's Office which serves as lead agency, participants include the Joint Terrorism Task Force; the FBI, Customs and Border Protection; U.S. Coast Guard, Immigration and Customs Enforcement; Secret Service, Transportation Security Administration, and other agencies. At the state and local level, the South Carolina Law Enforcement Division, the Charleston County Sheriff's Department, and the police departments of Charleston, North Charleston, and Mount Pleasant are involved in the project. Seahawk has linked databases and physical security systems that are designed to better screen ships, crews, itineraries and cargo manifests, as well as improve the physical security aspects of daily port operations in Charleston harbor. The physical security systems include video camera feeds, radar, and thermal imaging. The Project also serves as a test site for new maritime security equipment.

Project Seahawk is similar to Project Jayhawk (or JHOC for Joint Harbor Operation Center) that is currently being developed at the Ports of Norfolk, Virginia and San Diego, California. JHOC predates September 11, 2001. JHOC is a collaborative effort of the Navy and Coast Guard designed to provide a command, control, communications, computer and information system, and surveillance and reconnaissance capability at these two ports. The Ports of Norfolk and the Port of San Diego, in addition to handling commercial cargo, are also home to the two largest U.S. Naval stations. Preventing a *USS Cole*-style attack against Navy ships docked at these two naval stations was one

[12] Department of Homeland Security Fact Sheet: CBP Port Inspection and Surveillance Technologies, 2006

impetus for creating the JHOCs.[13] At Norfolk, the JHOC is staffed with Navy and Coast Guard personnel. It is housed in a Navy tower that overlooks the main shipping channel and is also equipped with radar and surveillance monitors. At San Diego, the JHOC is focused not only on protecting Navy ships, but other Coast Guard missions in the marine environment, such as drug interdiction, alien and migrant interdiction, environmental protection, and search and rescue. It is housed in a Coast Guard facility. Initially staffed with Navy, Coast Guard, and local harbor police personnel, it now also is staffed with Customs and Border Protection personnel.

The Coast Guard is evaluating these three operation centers as potential models for strengthening security at other U.S. ports. The Coast Guard has reorganized their authorities and responsibilities for a given port and its surrounding coastal area into command entities it calls "sectors." The existing JHOCs are viewed as a prototype for "sector command centers" under its reorganization plan. The Coast Guard plans to develop sector command centers at ten port locations, but may expand this to up to 40 port locations. The Coast Guard is currently conducting site visits to determine the best locations for sector command centers.

Created and funded within the Department of Justice, Seahawk takes the idea of the Joint Harbor Operation Center (JHOC) and streamlines the actors and the processes. When dealing with waterways there are many competing interests. Especially in a port with a large military presence, the coordination between the Navy, Coast Guard, CBP, and local law enforcement must be seamless. There are very few places where this is the case and at the Port of Charleston; although they are getting closer.

These operation centers appear to offer a mechanism for DHS and other law enforcement agencies to share information and coordinate responses in the seaport environment. A Government Accountability Office (GAO) review of these operation centers found that participants involved in them believed they offered a means to provide continuous information about maritime activities and involve various agencies directly in operational decisions using this information.[14] Participants noted that while the "Area Maritime Security Committees" required by MTSA provided a means to share information, they did not offer a means to coordinate security activities and did not do so on a day-to-day operational basis. The participants also believed the centers help

[13] A description of the USS Cole attack is provided in CRS Report RS20721, *Terrorist Attack on USS Cole: Background and Issues for Congress.*

[14] 05-394, *Maritime Security: New Structures Have Improved Information Sharing, but Security* Clearance Processing Requires Further Attention, April 2005, pp. 16-22.

leverage the resources and the authorities of the respective agencies by collaborating in vessel boardings, cargo examination, and enforcing security zones. For instance, if the Coast Guard was to board a vessel, other agencies could also send personnel to enforce the laws related to their jurisdiction.

Former Coast Guard Commandant Thomas Collins has asserted that "a robust sensor and command and control capability in the port … will be a significant contributor to achieving …future security initiatives."[15] In short, each port should have a Seahawk/JHOC. A virtual and physical integration and collaboration between entities has never been more important.

[15] Thomas H. Collins. Letter to the Honorable Don Young 12 April 2005.

Section III

Substantial Room for Improvement

Investment in Technology

Last April, the GAO published a report on the status of the Container Security Initiative (CSI), a program launched by U.S. Customs and Border Protection (CBP) in January 2002 to target and inspect high-risk cargo from foreign seaports before they depart to the United States. The GAO reported about 35 percent of the shipments from CSI ports were not targeted or subjected to inspections due to staffing issues.

The report also noted that CBP has limited assurance that inspections conducted are effective at detecting and identifying terrorist weapons of mass destruction because minimum technical requirements for detection equipment do not exist.

Experts believe that many of the technologies we need to prevent future attacks are at our fingertips and many others are already in place in various pilot programs or initiatives. For example, The Department of Energy through the National Nuclear Security Administration (NNSA) has worked to reduce global danger from weapons of mass destruction. Through the MegaPorts initiative, the DOE is able to monitor the shipping industry with radiation detection equipment, which specifically checks for nuclear or other radioactive materials.

The Integrated Container Inspection System (ICIS) is a pilot system at the Port of Hong Kong. It is able to scan 100% of containers in a particular lane, using three successive scanning machines. The system does not require the truck to stop or proceed at any slower rate than it does when normally moving through scanning equipment. This test program offers promising results; however, it remains expensive to operate and requires a significant increase in manpower. The $400 per hour rate is only for the machines to scan the images. That expense does not include the cost of employing CBP agents to analyze the information and image. Further, the time required to interpret the image produced by the scanning equipment is an average of four to six minutes per container. That is far too much time to feasibly scan and analyze every container at the Port without causing serious delays and backlogs in the movement of commerce. Further substantial investment in technological

improvements is required to speed the process and reduce costs before we could consider implementing 100% scanning.

Setting Higher Standards

Unfortunately, government and industry use many terms interchangeably which represent very distinct level of security, leading to confusion about the true level of threat protection "inspection" is different than "screening", which in turn is very different than "scanned". For instance, CBP asserts that they perform "100% inspection". To be clear, they inspect 100% of their paper or computer manifest of cargo, NOT the actual cargo. That is not sufficient. The manifest data may be in error, or worse, it may be falsified to hide a threat. Further, if 100% of cargo containers are scanned through an ICIS machine that alone is not security if 100% of the scans are not examined by a trained professional to detect threats.

In the ideal, 100% of manifests would be reviewed with a small percentage of them randomly matched against the corresponding container which is stopped, opened, and inspected. Suspect or questionable manifests would also trigger a physical inspection. Even then, 100% of containers should be scanned while a random number of containers, which passed the scan would be stopped, opened and inspected as both a deterrent as well as a check against innovation by terrorists finding new ways to subvert the scanning technology. Of course, any "negative scan" or questionable scan should trigger a physical inspection.

It is important to strive for a productive relationship with host country customs officials. If a container has been targeted for inspection, it is up to the host country to inspect. We have to make sure the host country's inspector is thoroughly and diligently inspecting the container. It takes a combination of intelligence, enough people on the ground, and the best technology available to achieve our goals. Our objective is to catch the problem before it gets to our shores. If it is in harbor, it is too late.

Transportation Workers Identification Card (TWIC)

A modern, electronic, tamper-proof identity card is an attempt to weed out possible threats to our ports by creating a layer of protection that ensures that workers have had background checks. By combining a background check with a biometric identification card, we can reduce the threat of an "insider" attack on one of our ports.

The Department of Homeland Security (DHS) has initially called for the implementation of the TWIC cards which involve background checks only, without requiring a scanning system which ensures the individual who possesses the card is in fact the cleared employee and not a terrorist.

DHS has apparently yielded to industry concerns that a single federal standard to require scanning of ID's throughout a port facility will require workers to physically touch readers and scanners in order to access work areas – slowing work and requiring an additional maintenance burden to support the scanning equipment. Terminal operators argue the port environment is busy and dangerous, and exposure to the elements make touch scanning impractical and will reduce worker productivity. Yet, the prevalence of wireless readers and technology should make it possible for the U.S. to solve this problem.

We have one note of caution. TWIC cards have the potential to allow for a building of profiles on workers. Such data might prove a useful tool for checking criminal history, immigration status, work records and a check of the terrorist database, it could also be used to track a worker's movements and habits. We must be careful to strive for a balance of protecting our homeland and maintaining our freedoms and liberties. This program could erode privacy by making it easier to track people to a degree that is unnecessary for security.

The Right Initiatives: C-TPAT, CSI & Mega Ports

There are three essential government initiatives which focus on global supply chain security. The Customs Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI) are both run out of CBP, and the Department of Energy's Mega Ports Initiative.

After 9/11 CPB redefined its mission and now operates on a mandate to intercept any threat to homeland security. To that end, C-TPAT was organized to create a public/private/international partnership with over 5,800 businesses, including most of the largest U.S. importers. The goal is to improve the security of the global supply chain in the private sector. The C-TPAT program allows CBP to designate certain companies as low risk, based on the company's past compliance history, security profile and validation of a sample international supply chain.[16] This affords the devotion of fewer resources on "certified" shippers so that CBP can put more resources at work on higher risk shippers.

[16] Department of Homeland Security. (2004). Securing the Global Supply Chain. Washington, DC: Office of Field Operations & Office of Policy and Planning.

This system allows for a smooth and effective way to rank shipments and shippers. It is not yet practical to scan all cargo and all shippers equally. It is not efficient to subject our partners to the same rigorous traps as those shipments which we suspect. In essence, C-TPAT is rewarding companies for being forthcoming and demonstrating good behavior. Those participants who prove a sustained commitment to safety requirements are rewarded.

Delays in Security Plan Evaluations Must be Remedied

Many in Congress have expressed a concern that CBP has been slow to effectively review applications for certification. On May 4, 2006 Representative Loretta Sanchez (D-CA) offered an amendment to H.R. 4954, the SAFE Port Act, which would prohibit the current CBP practice of granting automated targeting risk score reductions through C-TPAT for applicants who have not received CBP validation of the implementation and effectiveness of their security measures. The amendment failed 195 ayes, 203 nays, 7 not voting *(Roll No. 125).*

Debate on the amendment revealed that 5,000 companies have submitted written security plans and have received CBP certification. This certification allows shippers to be fast-tracked through our ports. However, only 1,200 companies have had their plans validated. To receive validation CBP visits the sites, thus ensuring the company has truly implemented the security measures in their security plan.

Working in tandem with C-TPAT is the Container Security Initiative (CSI). CSI screens high-risk containers in key ports overseas. CSI currently operates at 42 participating ports. By the end of 2006, the number is expected to grow to 50 ports covering more than 90% of cargo shipped to the United States.[17] The CSI ideally should facilitate the flow of trade and make processing faster for certain shipments and certain shippers. U.S. Customs inspectors are stationed at participating ports and are allowed to observe and verify inspections.

CSI has proved to be an effective program in as much as it anticipates problems and attempts to prevent them. By placing CBP agents at host ports via bilateral agreements, they can work with host country officers to decide which containers to target for inspection – based upon intelligence, information provided through C-TPAT, and other data sources, which help assess a given cargo's risk. It is the host country officers who inspect

[17] Department of Homeland Security. Fact Sheet: CBP Port Inspection and Surveillance Technologies (Washington, D.C. : GPO, 2006) 1.

suspicious containers through either imaging machines or through physical inspection.

One further notable program aimed at securing the global supply chain is run through the Department of Energy, under the Office of Second Line of Defense (SLD) and has been focusing on preventing nuclear smuggling since the end of the Cold War. The DoE program, Mega Ports, predates 9/11 and now works in consort with the Container Security Initiative to prevent nuclear smuggling by securing not only nuclear materials, but also the primary smuggling routes including seaports, land borders and airports.

Nuclear Threats must be addressed

There are two types of radiation threats we must monitor; dirty bombs and nuclear weapons (with associated components). The first, dirty bombs, are smaller, have less of a blast zone, and can be created using low grade nuclear material and many every day substances. If a dirty bomb was released on the island of Manhattan, only a small area (e.g., one building) would be damaged from the blast, but the area surrounding the blast site would be highly contaminated with potentially lethal levels of radiation. In addition, harmful levels of radiation would spread rapidly throughout the island.

Also of concern, is the potential ease with which dirty bomb materials can be obtained. Steven Flynn of the Council of Foreign Relations writes in his book *America the Vulnerable*, about the prevalence of radiological materials and how little we know about where they are. "The U.S. and Canada have over two million licensed sources of radiological materials, 500,000 of which are near or beyond the end of their service life. Three hundred sources of radiation have been reported as "lost" or "stolen" on an annual basis since 1996, 56 percent of which have never been recovered." [18]

It is critical to know where these materials are located within our country and more importantly, beyond our borders. While the U.S. and Canada have strict licensing regulations on who may handle, utilize and dispose of these materials, other countries do not. Detection of materials coming into this country is a critical layer of securing our nation.

Radiation portal monitors (RPM) and Radioactive Isotope Identifiers (RIIDS) detect and identify radiation emitted from materials hidden inside cargo containers. Both RPMs and the RIIDS are useful tools for providing levels and types of radiation. Unfortunately, first generation RPM's only tell us how

[18] Stephen Flynn, *America The Vulnerable*, (New York: HarperCollins Publishers 2004) 25.

much gamma or neutron radiation is present, leaving the more difficult assessment of "what type of radiation" to secondary inspectors using RIIDS. Those agencies tasked with securing our cargo such as CBP and DOE do not have enough basic or advanced technology equipment to gauge the amount, type, energy, frequency and characteristic of the radiation. Without this equipment, they have an uphill battle ensuring each container is secure, safe to transport, and admissible into the United States.

The second radiation threat, nuclear weapons and associated components, produces a far greater blast zone and can spread lethal levels of radiation across a much larger area. Effort aimed at combating this threat are focused on the smuggling of weapons grade nuclear material, such as plutonium or uranium, that can be assembled with other bomb components resulting in a viable nuclear weapon. The ramifications of such a weapon are unimaginable on many levels. Ensuring that nuclear components are not smuggled into this country must be a top priority for government, business and industry.

Detecting a nuclear component or weapon is difficult because of the stable nature of weapons grade "fissile" materials. Uranium filtered and refined to weapons grade U-235 emits few neutrons and subsequently is difficult to detect using the RPMs and RIIDS in widespread use today. Non-Intrusive Imaging (NII) systems take an "X-Ray" type picture of the cargo container to look for dense, dark spots that could be shielding, or a nuclear component.

Currently, radiation scanning and NII are performed in separate operations wasting valuable time, energy and resources. This waste significantly impacts an already over burdened shipping infrastructure. We must move forward to combine radiation scanning and NII into a single inspection system – a proverbial assembly line of security. The sooner we create a more comprehensive approach to scanning for both radiation and shielding, the sooner we will have a complete picture of our safety.

Section IV

Recommendations

Put Someone in Charge

C-TPAT and CSI is based on an assumption about participating shippers in that they are "good actors" in this agreement. These programs work because shippers provide layers of protection and filter out known bad actors. Congress and the Administration need to make sure we focus on the port of embarkation and providing the best intelligence available.

Our intelligence agencies have made strides in removing the stovepipes and creating a better integrated system of coordination and collaboration throughout the Intelligence Community. We need to make sure port and supply chain threats are a priority. The most effective tool to ensure we stop the terrorist action before it even makes it to the port of embarkation is actionable intelligence. The President, through the Director of National Intelligence and the Secretary of Homeland Security needs to have a senior executive level officer who is dedicated to looking for port threats across agencies and across functions. The President should designate a single officer in government who can compel CIA, DEA, DOD, DoE, FBI, CBP, Coast Guard, Customs and other federal agencies to share information and direct their response whenever a threat is identified.

Beef Up Collaboration

Joint Harbor Operation Centers (JHOCs) and Project Seahawk are clear examples of the type of collaboration necessary to keep our ports safe. Increasing collaboration between all stakeholders is essential. Collaboration allows a command to connect the dots and link together intelligence piece to paint a coherent and accurate picture of the threats a port may face. We recommend the continued build out of Project Seahawk and JHOC's at U.S. ports and urge the speedy deployment of these centers.

Some of the best intelligence comes from police officers on the street. We need to make sure that information is freely flowing up and down stream. The joint Operation Centers is a good step in that direction. DHS should take the lead in expanding these centers to make sure state, local governments, and private industry security share information. By sharing information we can

have an accurate assessment of our trading partners, host countries, groups and businesses who are associated and friendly with terrorist organizations, and we can create possible avenues of access for terrorist. We recommend that the DNI set up intelligence sharing within the intelligence community and the DNI should include and work with private port industry security and port employees to bring in all available intelligence.

We also need stronger relationships and more intelligence and information sharing with our trading partners. The best weapon against a terrorist or threats to our country is good intelligence. Good intelligence requires the cooperation of all parties involved. We recommend that the DNI establish a system and protocols to address global supply chain security intelligence with our trading partners.

Protocols for the Resumption of Trade

Threats to our ports affect many arenas. Obviously it affects commerce, and threatens the millions of Americans that live and work near our ports. It also has the potential threat of severely damaging other industries such as energy production and energy storage. We cannot look at this as just an attack on ports. It is an attack on a major lifeline to our communities and to our countries. Destruction of our ports can destroy energy facilities, warehoused goods, inter modal areas such as truck and train terminals, and obviously can be catastrophic loss of life.

Protocols need to be established, but they should include an assessment of impact to concentrated critical infrastructures. While it is vital to get the port up and running, we need to assess what other damage is done and how we make sure those other industries are not left holding the bag. We recommend Congress appoints a task force of government, industry, transportation services to build out plans to get a port up and running. Delays in the resumption of trade can cripple our economy.

Speed the Innovation and Implementation of New Technology

Technology is an essential part of securing our port and we have many expert private sector partners that are developing the latest in the war on terror. However, the federal government still has cutting edge technology and massive research capabilities that cannot be ignored. We also have catalogues of technology that must be made available for our homeland security.

This year Congress included language in the DHS Authorization bill to increase the sharing of technology from the Department of Defense to the Department of Homeland Security DHS. Sharing of technology, especially advanced screening technology, should not be limited to these two agencies.

Since 9-11 information sharing has been the new ethic throughout the Intelligence community. The Patriot Act and the Intelligence community reform sought to break down bureaucratic barriers to collaborative efforts in fighting the war on terror. Sharing technology is a part of that equation.

We recommend that Federal Departments and Agencies redouble their efforts at sharing technology and expertise so that we can move port security technology forward and into as many domestic and foreign ports as possible

Privacy Must Be Protected

We must concern ourselves with the abuses that can occur with technology. Technology gives security new levels of power and greater scopes of action; however, it also allows for a building of profiles on workers without their permission and without an understanding of what can be used against you in the future. We have to be careful and we have to achieve that balance of protecting our homeland and keeping our freedoms and liberties intact. We recommend that as we proceed with TWIC cards we strongly encourage privacy standards to be established, ensuring the sensitive and personally identifiable information kept secure with appropriate access by law enforcement when appropriate.

Summary of Recommendations

- The President should put a senior officer in government in charge of Port and Global Supply Chain Security.
- The DNI and the Secretary of Homeland Security should create a senior level executive in each agency to oversee and coordinate port and global supply chain security intelligence.
- The DNI should establish a program to watch over Port Security intelligence and to train analysts to understand this threat.
- The DNI should enhance intelligence sharing with local law enforcement and should include and work with private port industry security and port employees to bring in all available intelligence.
- The DNI should establish systems and protocols to address port and global supply chain security intelligence with our trading partners.

- Congress should direct and fully fund an expedited build-out of Project Seahawk and JHOC's at all U.S. ports.
- Congress should appoint a task force of government, industry, transportation services to establish a process to determine protocols to get a port up and running after an incident.
- All Federal Departments and Agencies should redouble their efforts at sharing technology and expertise so that we can move port security technology forward and into as many domestic and foreign ports as possible.
- DHS should speed the development of a TWIC program, including a system of wireless readers in our ports.
- DHS should implement TWIC cards but we strongly encourage that privacy standards be established to ensure the sensitive and personally identifiable information be kept secure with appropriate access by law enforcement.
- The President should direct an assessment of all strategic ports world-wide, and complete a timeline of implementing port security screening technology.