# Port Security Neg

## \*\*\*Case Answers\*\*\*

### Frontline – AT: Ports Vulnerable

#### **1. Squo solves- two bills JUST passed**

States News Service, June 6, 2012, “TWO CRITICALLY IMPORTANT PORT SECURITY MEASURES SPONSORED BY CONGRESSWOMAN LAURA RICHARDSON INCLUDED IN NEW HOMELAND SECURITY BILL RICHARDSON AMENDMENTS ENABLES PORT SECURITY GRANT RECIPIENTS TO USE FUNDS TO MODERNIZE EQUIPMENT AND TO PAY COSTS OF SECURITY PERSONNEL,” lexis)

The House Homeland Security Committee today approved a bill that includes two critical measures sponsored by Congresswoman Laura Richardson to strengthen port security. "I have met with many ports authorities and port security grant recipients who have expressed to me their frustration with current rules that hamper their ability to maximize port security," said Congresswoman Laura Richardson. "I agree with these port experts that it does not make sense to require grant recipients to fix security equipment when it may be cheaper to replace it with newer improved technology," said Congresswoman Richardson. The Congresswoman's Port Security Equipment Improvement Act was accepted as an amendment to the SMART Port Security Act (H.R. 4251). By including this amendment Port Security Grant Program recipients will now be permitted the flexibility to determine whether it is more cost-effective to use funds to replace or maintain security equipment. Previously, Port Security Grant Program funds were to be used solely for maintenance of security equipment, but not for equipment replacement. Congresswoman Richardson also successfully worked to include her Port Security Boots on the Ground Act (H.R. 5803) in Section 107 of the SMART Port Security Act. Because of this amendment security personnel costs will be permitted to be covered through grant funding. Currently, Port Security Grant Program (PSGP) funding cannot be used to fund statutorily-mandated security personnel costs yet this spending prohibition only exists for the ports. "American ports should not have to bear the burden of protecting our most vital stream of commerce and source of American jobs on their own," said Congresswoman Richardson. "Instead, ports should be allowed to utilize PSGP grants to hire and pay current security personnel who are used to staff fusion centers, emergency operations, and counterterrorism posts," said Congresswoman Richardson. The Congresswoman's proposal to amend the bill to include security personnel costs to be funded through grants passed with unanimous consent. To keep funding regulated, the amendment also places a cap on the amount of PSGP funding that can be used to pay security personnel costs. Payments will be limited to 50 percent of the total amount awarded to grant recipients in any fiscal year.. "

#### 2. Squo solves – no terrorist attacks on a U.S. Port ever and billions of dollars are already being spent on port security.

Ingle 8-18-08 (Laura Ingle, Correspondent and reporter for FOX News, “U.S. Patrols 300 Ports of Entry, Potential Terrorist Gateways”, FOX News, <http://www.foxnews.com/story/0,2933,405822,00.html>)

NEW YORK — There are over 300 official ports of entry in the United States, giant pores where billions of dollars worth of goods flow through every day — giant targets for terrorists seeking to smuggle in weapons for the next attack. U.S. Customs and Border Protection is the first line of defense, scouring for so-called "dirty bombs" and other weapons of mass destruction. "Our strategy begins with stationing our officers overseas, and we have over 200 Customs and Border Protection officers around the world in 58 of the largest seaports," said Jay Ahern, deputy commissioner of U.S. Customs and Border Protection. The idea is to "push the borders out" — to have more control of imports and more time to manage potential terror threats before they head to U.S. shores. All incoming cargo ships are checked electronically, and all crews and cargo are accounted for and logged. In addition, all vessels coming from foreign ports are boarded by customs agents to make sure that everything that was screened prior to arrival still checks out. There has never been a terrorist attack on a U.S. port, and since the Sept. 11 attacks, billions of dollars have been spent on homeland security, but some critics say more needs to be done.

#### 3. High risk cargo gets checked now

Wolf, 09/13/2006[Bryon Wolf, Political Editor and Deputy Political Director for abc news , ÔøΩHow much is too much for Port Security?,ÔøΩ world news, <http://abcnews.go.com/US/Politics/story?id=2425748&page=1#.T-Hnc47wefQ>]

For Now, Limited to "High Risk" Cargo. Currently, port screening includes the identification of high-risk cargo by checking shipping manifests.Importers must provide manifests before their cargo can be brought into the United States.The Department of Homeland Security then uses the information to better target high-risk cargo. The new bill would authorize this process, which is already being used.

#### 4. Tech improvements solve.

Ituh, International Trade Specialist @ Aurora Networks, Inc, 2010 (Archibong J., “Port Security Technology for Closed Container Inspection at United States Seaports of Entry” Feb. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/10209/Ituh-2010.pdf?sequence=1)

The potential threat of terrorists using containers as a way to smuggle a nuclear or radiological device inside a cargo container poses a large risk to our economies and to our societies (van de Voort, O’Brien, Rahman, & Valeri, 2003). The current technologies being used at the seaports of entry to detect dangerous cargo are not perfect or foolproof, but they are steadily improving in accuracy and reliability. Non-intrusive (gamma and x-ray) technology provide the capability to image the contents of containers without opening them. This technology is widely used and has benefited customs inspectors, but requires significant human operator involvement (Unisys Corp, 2007). Radiation detection technology is also a key tool, but is hampered by nuisance alarm rates that reduce its effectiveness. None-the-less, there are documented benefits of radiation scanning to government entities, including port authorities and customs inspectors, which include: (a) prevention of an act of terrorism, (b) meeting mandates and requirements established by domestic government entities for the radiation scanning of containers, and (c) providing assurances to the local community and port workers as to the security of cargo containers (Unisys Corp, 2007).

### EXT – Ports Secure Now

#### Port Security is high now and doesn’t hamper international trade.

Ituh, International Trade Specialist @ Aurora Networks, Inc, 2010 (Archibong J., “Port Security Technology for Closed Container Inspection at United States Seaports of Entry” Feb. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/10209/Ituh-2010.pdf?sequence=1)

According to Banamyong (2005), security measures are necessary to guarantee the protection of global supply chains against acts of terrorism or any possible unexpected threats. Since September 11, 2001, the United States has pursued a layered approach to port security intended to ensure the integrity of the supply chain from the point of container loading to the arrival in the United States without hindering the flow of commerce through ports (Langhoff & Pillai, 2007). Under the layered security system, the United States Customs and Border Protection (CBP) determines risk by carefully analyzing various data sources including ship and cargo manifest information on shippers and cargo points of origin, as well as classified intelligence. These capabilities provide CBP and other federal agencies the intelligence they need to make informed decisions regarding the level of cargo risk, determine which merit additional scanning and investigation, and help get information to the field personnel (Langhoff & Pillai, 2007).

#### Port Security is high now – multiple measures

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

The potentially catastrophic consequences of terrorist misuse of the trading system mean that its security must be a U.S. priority. And Washington has taken steps to address the threat. Since the attacks of 2001, the number of inward-bound cargo containers inspected by Customs (across all modes of transportation) has risen by nearly two-thirds, from 7.6 percent to 12.1 percent of the total. For sea containers, the increase has been from 2 percent to 5.2 percent. 11 In addition, DHS has begun implementing new programs and procedures—the 24hour rule, the Custom-Trade Partnership against Terrorism, the Container Security Initiative, Operation Safe Commerce, and others— designed to safeguard the transportation and supply chains. The goal, according to policymakers, is to “push the border outward” by decreasing the chances of terrorist infiltration of trade networks before goods ever arrive in the United States. Robert Bonner, commissioner of the new U.S. Customs and Border Patrol, put it this way: We can no longer afford to think of ‘the border’ merely as a physical line separating one nation from another. We must also now think of it in terms of the actions we can undertake with private industry and with our foreign partners to prescreen people and goods before they reach the U.S. The ultimate aims of ‘pushing the border outward’ are to allow U.S. Customs more time to react to potential threats—to stop threats before they reach us—and to expedite the flow of low-risk commerce across our borders.12

### AT: Ports Vulnerable – Congress Solves

#### S. Quo Solves – Actions already being taken in order to increase Port Security; examples like the MTSA and Port Security Act prove.

Caldwell, 10-30-07 (Stephen L. Caldwell, Director of Homeland Security and Justice Issues, “MARITIME SECURITY The SAFE Port Act: Status and Implementation One Year Later”, GAO, <http://www.gao.gov/new.items/d08126t.pdf>)

Since the 9/11 attacks, Congress has established a new port security framework—much of which was set in place by the Maritime Transportation Security Act (MTSA)2. Enacted in November 2002, MTSA was designed, in part, to help protect the nation’s ports and waterways from terrorist attacks by requiring a wide range of security improvements. Among the major requirements included in MTSA were (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; (3) developing the Transportation Worker Identification Credential (TWIC), a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishing of a process to assess foreign ports, from which vessels depart on voyages to the United States. The Department of Homeland Security (DHS)—itself a creation of the new security environment brought on by the 9/11 attacks—administers much of this framework, which also attempts to balance security priorities with the need to facilitate legitimate trade. The SAFE Port Act, which was enacted in October 2006, is one of the latest additions to this port security framework. The act made a number of adjustments to programs within this framework, creating additional programs or lines of effort and altering others. The SAFE Port Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA. The SAFE Port Act included provisions that (1) codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), two programs administered by U.S. Customs and Border Protection (CBP) to help reduce threats associated with cargo shipped in containers, as well as established the Domestic Nuclear Detection Office (DNDO), which is responsible for conducting research, development, testing, and evaluation of radiation detection equipment; (2) required interagency operational centers where agencies organize to fit the security needs of the port area at selected ports; (3) set an implementation schedule and fee restrictions for TWIC; (4) required that all containers entering high-volume U.S. ports be scanned for radiation sources by December 31, 2007; and (5) required additional data be made available to CBP for targeting cargo containers for inspection. This statement summarizes our recently completed and ongoing work

#### U.S. and other countries ports already safe

U.S. Environmental Protection Agency, July 18, 2010,[U.S. Environmental Protection Agency, EPAÔøΩs Clean Material Program, ÔøΩShipping Port SecurityÔøΩ, RadTown USA, <http://www.epa.gov/radtown/port-security.html>]

The **Federal government** also **developed** and **implemented** an enhanced **strategy to identify, target, and inspect cargo containers *before* they reach U.S. ports**. Officials prescreen all cargo, and any shipment that poses a potential threat is physically inspected with radiation detectors either prior to or upon arrival.

The **U.S. government created a partnership with** over 7,000 businesses, including **most of the largest U.S. importers**. **Under this** partnership program, legitimate companies that conduct regular business with t**he U.S. have increased their own security to prevent terrorists** from infiltrating their shipments. This system of prevention, early detection **and** immediate action helps **keep our ports safe from terrorist threats**.

#### Govt already invests a lot to make ports secure

APPA, 12 (APPA, serves and assists educational institutions throughout the United, “10 Years After 9/11, Security Still a Top Priority of U.S. Ports”, The Maritime Excutive, <http://www.maritime-executive.com/article/10-years-after-9-11-security-still-a-top-priority-of-u-s-ports>)

In the decade since Sept. 11, 2001, America’s seaports and the federal government have joined forces to make major gains in fortifying and hardening port facilities against intruder attack. Since then, public port authorities have made terrorism detection and prevention one of their top priorities. With the combined efforts of port authorities and initiatives of federal agencies within the FBI and Department of Homeland Security (DHS), including the U.S. Coast Guard, Customs and Border Protection (CBP), Transportation Security Administration (TSA), Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement and the Domestic Nuclear Protection Office, ports are significantly safer now than prior to 9/11. He added, “With the death of Bin Laden, critical infrastructure facilities, such as ports, are being asked to be extra vigilant to protect against retaliatory terrorist attacks.  In addition to making continued enhancements, the Port Security Grant Program helps pay for maintaining and replacing our current security assets at ports.” The comprehensive Maritime Transportation Security Act (MTSA) of 2002, and the Security and Accountability For Every (SAFE) Port Act of 2006 changed the way ports handle cargo and passenger movements.  To implement the security measures in this legislation, America’s ports and their terminal operators have invested billions of dollars into security personnel and training, enhancements to perimeter security, access control and credentialing systems, interoperable communications technology, and waterside security such as patrol boats, vessel tracking and underwater threat detection systems. The industry also maintains ongoing liaison with the federal government’s lead port and maritime security agencies.  These dialogues address timely security issues such as the Transportation Worker Identification Credential (TWIC), which the TSA and Coast Guard implemented 2007 to ensure those seeking access to secure port areas can be positively identified, have authorization to enter the facility and do not pose a terrorist risk. In concert with public port authorities and terminal operators, the Coast Guard is charged with routinely inspecting and assessing the security of U.S. port facilities and the vessels that call those facilities, in accordance with the MTSA and the International Ship and Port Facility Security Code.  Since 9/11, the Coast Guard has instituted innovative programs such as Maritime Safety and Security Teams, enforced security zones, increased its intelligence gathering and analysis capabilities, expanded its partnerships with the maritime industry, international organizations, federal, state and local agencies, and has joined with other agencies within DHS to strengthen U.S. borders and protect America’s ports and waterways.  The Coast Guard also cross-checks crew lists against terror watch lists in advance of arriving ships. Additionally since 9/11, CPB has initiated: the Container Security Initiative to examine high-risk, U.S.-bound containerized cargoes at foreign ports; the 24-Hour Rule, which requires cargo manifests be submitted a least a day ahead of ship arrivals; C-TPAT which provides expedited inspections for U.S. importers that voluntarily work with CBP to improve baseline security standards for supply chain and container security; and large-scale X-ray, gamma ray and radiation detection devices at U.S. ports to scan the contents of inbound cargo containers. Since 9/11, the Port Security Grant Program has received about $2.6 billion in funding for 11 rounds of grant awards.  *AAPA commends Congress and the Administration for these allocations and will continue to recommend the federal government commit $400 million a year for a separate and dedicated program to help port facilities enhance their physical security.  The association supports a risk-based evaluation process that allows all facilities that are required to meet MTSA regulations to apply.* “Clearly, America’s ports have become much more secure since 9/11. In addition to guarding against cargo theft, drug smuggling, human trafficking and stowaways, ports and their law enforcement partners have added the protection of people and facilities from terrorism to their security plate,” remarked Mr. Nagle. *“There’s no question* that more investments in security equipment, infrastructure, technology, personnel and training will be needed. All parties—the ports, terminal operators, the various government agencies, and the Administration and Congress—must do their part in undertaking and funding these enhancements.  Only by continuing to make port security a top priority will America’s seaports be able to continue serving their vital functions as trade gateways, catalysts for job creation and economic prosperity, and important partners in our national defense.”

#### SAFE Port Act would solve

APPA, 12 (APPA, serves and assists educational institutions throughout the United, “10 Years After 9/11, Security Still a Top Priority of U.S. Ports”, The Maritime Excutive, <http://www.maritime-executive.com/article/10-years-after-9-11-security-still-a-top-priority-of-u-s-ports>)

AAPA is strongly in favor of reauthorizing the SAFE Port Act to ensure that U.S. port facilities and cargoes remain secure.  One such bill, S. 832, was introduced in April by Sens. Susan Collins (R-ME) and Patty Murray (D-WA), which would authorize $300 million a year for five years for the Port Security Grant Program and reauthorizes, among other aspects of the original bill, the Container Security Initiative, C-TPAT and the Automated Targeting System to identify high-risk cargo.

#### Steps have been taken to improve security

Rundle ’09 (Elaine Rundle. Elaine Rundle is a staff writer at Government Technology magazine. “Port Security Improves With Nonintrusive Cargo Inspection and Secure Port Access.” Emergency Management. http://www.emergencymgmt.com/infrastructure/Port-Security-Improves-With.html)

During the past eight years, port security has evolved to include new technologies and regulations. Ports also have been identified as part of the nation's critical infrastructure, and innovative steps have been taken to ensure their safety. "To a degree, it's like screening passengers in that you're looking for the needle in the haystack of what bad things could exist out there -- anywhere from radiation types of materials to an actual nuclear device to a bioweapon," said Eric Holdeman, consultant and former director of the King County, Wash., Office of Emergency Management. Ports are a unique environment to secure. They are open environments by nature because cargo can't move unless people have access to the terminals, Rooney said. Security involves not only the port facility, she said, but also the vessels and waterways. Coordination is a key facet of port security because the responsibilities for different components -- like facilities, vessels and crew member security -- reside with different partners.

Security Paradigm Shift. Before 9/11, Rooney said physical security at ports was minimal. Many ports -- including The Port Authority of New York and New Jersey -- lacked security professionals and instead were monitored by a law enforcement agency that covered traditional criminal issues. She said the N.Y. /N.J. port still has a Port Authority Police Department, but positions have been added to develop infrastructure security, emergency management planning and security plans. "[Pre-9/11] it was more the tactical security and law enforcement as opposed to the strategic planning and the day-to-day operational stuff," Rooney said. The Maritime Transportation Security Act that former President George W. Bush signed went into effect July 1, 2004, spearheaded more port security changes. "We were required to conduct assessments, write facility security plans, appoint facility security officers, and then comply with a set of performance-based regulations for securing your perimeter, controlling access, monitoring activities, and screening and inspecting cargo, vehicles and personnel," Rooney said. The act also required the establishment of Area Maritime Security Committees that include federal, state and local government entities and the boating industry. The committees collaborate on port security plans and ensure cohesiveness among stakeholders. For The Port Authority of New York and New Jersey, this meant collaboration among private companies that each had an every-man-for-himself security philosophy, Rooney said. "Coordinating 190 private companies and 50 or 60 federal, state and local agencies was very difficult, but we achieved it through the Area Maritime Security Committee," she said. "We took another step through this committee and wrote what we called the Portwide Strategic Emergency Management Plan." It was completed about four years ago and allowed the entities to stop competing for funding and focus on the port's most serious security risks.

### AT: Ports Vulnerable – Customs Solves

#### Customs enacting viable container security plan

GAO**,** July 25, **200**3 (GAO, U.S. General Accountability Office, “CONTAINER SECURITY Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,” GAO Office/Government Products, http://www.gao.gov/new.items/d03770.pdf)

Customs developed CSI and C-TPAT in response to security vulnerabilities created by ocean container trade and to the concern that terrorists could exploit these vulnerabilities to transport or detonate WMDs in the United States. Announced in January 2002, CSI allows U.S. Customs to screen containers at CSI-designated foreign seaports. Placement of a CSI team overseas allows Customs to work with foreign customs officials to identify and examine high-risk containers prior to their arrival at U.S. ports. Customs initially targeted the top 20 foreign ports that shipped 66 percent of total containers to the United States for CSI inclusion, and then expanded the program to additional strategic ports. In November 2001, Customs initiated C-TPAT to improve the security of containers as they move through the global supply chain. Under C-TPAT, Customs officials work in partnership with private industry, reviewing supply chain security plans and recommending improvements. In return, C-TPAT members receive the benefit of a reduced likelihood that containers traveling along their supply chains will be inspected for WMDs. For fiscal year 2003, the CSI budget is about $28 million, and the C-TPAT budget is about $9 million. These budgets combined are expected to increase to more than $73 million for fiscal year 2004 as the programs expand. During the first year, Customs quickly designed and rolled out CSI and C- TPAT, modifying operations over time. Customs achieved strong participation among the countries and companies, respectively, that it sought to enroll in CSI and C-TPAT. In CSI’s first year, Customs reached agreement with 15 governments to place Customs personnel at 24 ports and placed four or five-member CSI teams in 5 of these ports. In C-TPAT’s first year, more than 1,700 companies agreed to participate in the program, and most received the key benefit, a reduced likelihood of inspections for WMDs. As participation in these programs grew, Customs implementation evolved in response to challenges as they arose. For example, the first CSI team deployed in Europe discovered that critical information that it needed from the host customs administration was not readily available and, as a result, the CSI team was unable to achieve its goal of thoroughly screening containers overseas. To address this challenge, Customs implemented a “24-Hour Rule” requiring carriers to supply key information directly to Customs. Similarly, Customs initially expected that its account managers, who had experience working with the trade community, would recruit new C-TPAT members and assist companies with the development of their action plans. However, Customs later realized that C-TPAT needed staff with greater knowledge of supply chain security to help with the action plans as well as assist with other program elements. In response, Customs created a new supply chain specialist position, which was announced in May 2003. These supply chain specialists will play a key role in implementing critical program elements designed to ensure that member companies are improving and maintaining supply chain security practices.

#### US Customs has recognized the changing terrorism and taken steps to prevent problems

Romero ’03 (Jessica Romero. Jessica Romero has a BA from Florida State Univeristy; JD Candidate 2004, University of Chicago. “Prevention of Maritime Terrorism: the Container Security Initiative.” Chicago Journal of International Law 4.2)

The United States has shifted away from reactive counterterrorism law enforcement methods towards more proactive techniques to fight international terrorism. This shift is a result of the changing nature of the terrorist threat overseas, against which the US has now employed preventative diplomatic, economic, military, and legal strategies. The Container Security Initiative ("CSI") is a Bureau of Customs and Border Protection ("US Customs")1 program designed to prevent containerized shipping-the primary means of transporting goods in global trade-from being exploited by terrorists.2 CSI is an excellent illustration of contemporary evolving preventative legal strategies in the international arena. Under CSI, US Customs has entered into bilateral agreements with foreign governments to identify high-risk cargo containers and prescreen those containers for terrorist weapons at the port of departure instead of at the port of arrival.3 This Development addresses the changing nature of international terrorism, specifically in the context of maritime activity, and its impact on law enforcement agencies and other nontraditional antiterrorism actors such as the maritime shipping industry.

#### S. Quo Solves – No need for increased port security, top white house officials already fixed it.

Powell, 9-08-11 (Stewart Powell, Politics Interviewer for Chron, “Top White House Officials says Port Security has Been Improved”, Chron, <http://blog.chron.com/txpotomac/2011/09/top-white-house-official-says-port-security-has-been-improved/>)

The top White House official responsible for protecting the nation against follow-on al-Qaida attacks says there have been “a number of very important improvements” in security at maritime ports such as the 52-mile Houston Ship Channel since the 9/11 attacks a decade ago. John Brennan, President Obama’s counter-terrorism adviser, said the administration has effectively extended U.S. maritime borders to ports around the world by requiring U.S.-bound ships from countries with ties to terrorism to undergo pre-departure security screening.

### AT: Ports Vulnerable – Funding Increase

#### Non- Unique- we have seen a funding increase of more than 700 percent since 9/11

US Customs and Border Protection ’06 (USCP, Department of Homeland Security, 7/12/2006, “An Overall Picture of Port Security”, CBP.gov, <http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/port_security/securing_us_ports.xml>)

Port security has been dramatically strengthened since 9/11. Funding has increased by more than 700 percent since September 11, 2001. Funding for port security was approximately $259 million in FY 2001. DHS spent approximately $1.6 billion on port security in FY 2005. Following 9/11, the federal government has implemented a multi-layered defense strategy to keep our ports safe and secure. New technologies have been deployed with additional technologies being developed and $630 million has been provided in grants to our largest ports including $16.2 million to Baltimore; $32.7 million to Miami; $27.4 million to New Orleans, $43.7 million to New York/New Jersey; and $15.8 million to Philadelphia.

### AT: Ports Vulnerable – PSGP Solves

#### Non- Unique- PSGP already funds Port Security- has money now

FEMA 2/17 (US Department of Homeland Security, government division, “FY 2012 Port Security Grant Program”, FEMA, <http://www.fema.gov/government/grant/psgp/>)

Port Security Grant Program (PSGP) Total Funding Available **in FY 2012:** $97,500,000 **Purpose:** PSPG provides funding for transportation infrastructure security activities to implement Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and state and local government agencies required to provide port security services. The purpose of the FY 2012 PSGP is to support increased port-wide risk management; enhanced domain awareness; training and exercises; expansion of port recovery and resiliency capabilities; and further capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices (IEDs) and other non-conventional weapons; and competitively award grant funding to assist ports in obtaining the resources required to support the National Preparedness Goal’s (NPG’s) associated mission areas and core capabilities.

#### Non-Unique- PSGP already funds Port Security

US DOT 2009

(Susan Lee, Maritime Administration Program Manager, “Port Security Grant Program”, US Department of Transportation Maritime Division, <http://www.marad.dot.gov/ports_landing_page/infra_dev_congestion_mitigation/intermodal_transport_networks/intermod_trans_net_port_sec/PSGP.htm>)

Since September 11, 2001, the U.S. Congress has appropriated over $2 billion for competitive grants to U.S. seaports to finance the cost of enhancing national port security. The purpose of the Port Security Grant Program (PSGP) is to help defray the costs of implementing the Maritime Transportation Security Act of 2002 (MTSA), which created new statutory requirements in port and vessel security. When it implemented the new MTSA regulations in July 2003, the U.S. Coast Guard estimated the private sector costs of compliance to be $6.8 billion over 10 years: $5.4 billion for port facility security and $1.4 billion for vessel security. The grant program is structured to be a shared responsibility between the federal government and the private sector, with applicants required to pay 25-50 percent of projects’ costs. This partnership between federal and private interests is crucial to make the U.S. more secure. Port Security Grant Program partners include the U.S. Department of Transportation’s Maritime Administration and several agencies in the U.S. Department of Homeland Security (DHS): the Federal Emergency Management Administration (FEMA), which administers the PSGP; the U.S. Coast Guard; and the Transportation Security Administration (TSA). The Maritime Administration has played a key role in the grant program since its inception in 2002. It is the only non-DHS agency involved in the program. Unlike its partner agencies, the Maritime Administration brings a commercial viewpoint to the application review and approval process. It also is the principal federal agency in the process that considers the impact of security measures on commerce. The Maritime Administration’s regional offices and headquarters have been actively involved in the grant program, reviewing and rank ordering applications and recommending funding levels and making policy recommendations.

### AT: Ports Vulnerable – US Won’t Cooperate Internationally

#### Their study is flawed, and cooperation will always be limited by sovereignty they can’t solve

Ituh, International Trade Specialist @ Aurora Networks, Inc, 2010 (Archibong J., “Port Security Technology for Closed Container Inspection at United States Seaports of Entry” Feb. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/10209/Ituh-2010.pdf?sequence=1)

The study does not provide for or cover movement of cargo between nations, the costs to businesses due to disruptions associated with the screening process other than its effect on delays to the international supply chain. A significant limitation associated with the screening is the lack of direct control of outbound cargo destined for United States seaports. Specifically, this pertains to the cooperation of foreign governments, and the issue of national sovereignty hinders and limits the desire of the United States Customs Service to place its officers, inspectors and inspection equipment at these foreign ports. To address this, the Container Security Initiative (CSI) program was developed by the United States Customs Service to encourage enhanced security arrangements and agreements between the United States and specific trading partners.

#### You can’t solve – requires cooperation form abroad

GOSLIN, Vice President of International Operations for Duos Technologies, Inc., is an international expert in security threat and risk assessment, 11/12/2008 (CHARLES “MARITIME AND PORT SECURITY” WHITE PAPER Dous Technology Inc. http://www.duostechnologies.com/DownloadCenter/WP-MaritimeAndPortSecurity.pdf)

Globally, there are very few uniform standards for point-to-point control of security on containers, cargoes, vessels or crews - a port’s security in one nation remains very much at the mercy of a port’s security, or lack thereof, in another nation. Organized crime is entrenched in many ports 2 , and a large majority of them still do not require background checks on dock workers, crane operators or warehouse employees. Most ports lease large portions of their facility to private terminal operating companies, who are responsible for their own security. The result of this is a “balkanized”, uneven system of port security and operations management as a whole.

### AT: Port Security Undermines International Trade

#### Port Security is high now and doesn’t hamper international trade.

Ituh, International Trade Specialist @ Aurora Networks, Inc, 2010 (Archibong J., “Port Security Technology for Closed Container Inspection at United States Seaports of Entry” Feb. https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/10209/Ituh-2010.pdf?sequence=1)

According to Banamyong (2005), security measures are necessary to guarantee the protection of global supply chains against acts of terrorism or any possible unexpected threats. Since September 11, 2001, the United States has pursued a layered approach to port security intended to ensure the integrity of the supply chain from the point of container loading to the arrival in the United States without hindering the flow of commerce through ports (Langhoff & Pillai, 2007). Under the layered security system, the United States Customs and Border Protection (CBP) determines risk by carefully analyzing various data sources including ship and cargo manifest information on shippers and cargo points of origin, as well as classified intelligence. These capabilities provide CBP and other federal agencies the intelligence they need to make informed decisions regarding the level of cargo risk, determine which merit additional scanning and investigation, and help get information to the field personnel (Langhoff & Pillai, 2007).

### AT: Terrorism

#### Upgrading security won’t help solve terrorism assaults on the US

Shie**,** October, 14, 2004**, (**Tamara Renee Shie, Tamara Renee Shie received her masters in International Policy Studies from the Monterey Institute of International Studies in August 2004. She also holds a MA in Southeast Asian Studies from the National University of Singapore where she studied while on a David L. Boren National Security Education Program fellowship. She served as a visiting fellow at the Pacific Forum CSIS in Honolulu, Hawaii from February to July 2004. Currently she is a research assistant at the Institute for National Strategic Studies (INSS) at the National Defense University (NDU) in Washington, D.C., “Ships and Terrorists – Thinking Beyond Port Security,” CSIS, <http://csis.org/files/media/csis/pubs/pac0445a.pdf>)

First, the emphasis on upgrading the security of major ports neglects the fact that these represent only a single link in the transportation chain. A shipping container may pass through some 15 physical locations and some two dozen individuals and/or companies while traveling from departure point to destination. Because containers are only searched at the major port, there is no guarantee they cannot be way laid in route after that point. Second, the CSI conducts security checks only on U.S.- bound containers. Therefore even if a tampered container arrives at a major port, if it is destined for a port other than the U.S., it is more likely to escape notice. Containers between the major ports of Singapore and Shenzhen or Pusan and Hong Kong are not subject to CSI requirements. Yet terrorist assaults on U.S. ships or interests can occur outside the U.S. Third, as major ports increase security, terrorists will look for other maritime targets or other means to target those ports. Terrorists are increasingly aiming at soft targets. Attacking maritime targets has never been particularly easy, often requiring a greater sophistication in planning, training, and coordination than those aimed at many land-based facilities. This is why maritime terrorism is rather rare, and why terrorists are less likely to attack a more secure major port. Yet in considering maritime terrorist threat scenarios – using a ship to smuggle goods or weapons, sinking a vessel in a major shipping thoroughfare, using a ship as a weapon, or even targeting maritime vessels – none require access to a major port or a shipping container to carry out a strike. There remain numerous small ports and small vessels not covered under the new security initiatives**.** The ISPS Code for instance only covers ships of 500 tons or more and port facilities that serve large international-bound vessels. The Code would not have protected the USS Cole.

#### Terrorists won’t put bombs in containers

Carafano and Quartel 7-5-2006 (James Jay Carafano, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies and Director, Douglas and Sarah Allison Center for Foreign Policy Studies; and Robert Quartel, former Member of the US Federal Maritime Commission, and an internationally recognized expert in international maritime and US national transportation policy. He currently serves as Chairman and CEO of FreightDesk Technologies, a leading provider of internet-based applications for international cargo management to shippers and Third Party Logistics Suppliers (3PLs); “Contain yourself”, The Heritage Foundation, <http://www.heritage.org/research/commentary/2006/07/contain-yourself>)

Some politicians want to require inspectors to look inside each container before it's shipped to U.S. ports. Supposedly, this would prevent terrorists from smuggling in a weapon of mass destruction or a "dirty" bomb (a large, conventional explosive laced with radiological material). But in reality, we'd be wasting our time and money. While it's true that a terrorist could put a bomb in a box, it's neither likely nor logical. In the case of all but a nuclear device, it would be easier and more certain to just build the weapon here. That's especially true for conventional explosives. Biological weapons can be produced with materials and equipment bought off the Internet or shipped here via any number of cargo delivery services. Potential chemical weapons surround us: chlorine tankers, gasoline trucks, pipelines and storage facilities. All a terrorist group needs for a dirty bomb is some low-grade radioactive material stolen from a hospital or a watch factory. Even the machines used to scan containers have radioactive material. Besides, if terrorists had a nuclear weapon, it's not at all clear why they would risk allowing it to leave their control. After all the time and trouble required to build a bomb, would they really wave good-bye and hope it gets to the right place? The terrorists would be far better off to hide their bomb in a private vessel (if they can afford a nuclear weapon, they can afford a boat to carry it in), a truck coming across from Canada, or a small tramp ship operating out of the Caribbean destined for, say, the Port of Richmond. If terrorists wanted to target a port, they would more likely use a truck, train or small boat. A McVeigh-style truck bomb, constructed domestically, would do the trick. And it would be much easier to approach a port from the land than from the sea. Finally, if foreign ports did attempt to screen every container of sneakers coming to America, they would likely fail. There aren't enough people and computers to scrutinize the millions of records that would be produced in real time before the containers reach their destination. It also isn't clear if any technology is fast, accurate and cheap enough to do the job with any degree of confidence.

#### Investing in port security won’t thwart terrorists, dangerous and false security

Kochems and Carafano 5-5-2006 (Alane Kochems, policy analyst for national security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation; James Jay Carafano, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies and Director, Douglas and Sarah Allison Center for Foreign Policy Studies; “One Hundred Percent Cargo Scanning and Cargo Seals: Wasteful and Unproductive Proposals”, The Heritage Foundation, <http://www.heritage.org/research/reports/2006/05/one-hundred-percent-cargo-scanning-and-cargo-seals-wasteful-and-unproductive-proposals>)

These approaches are efforts to thwart a nuke-in-a-box scenario, but the nuke-in-a-box is an unlikely terrorist tactic. If an enemy wanted to smuggle a bomb into the United States, an oil or chemical tanker, roll-on/roll-off car carrier, grain or other bulk vessel, or even private watercraft would be a more logical and secure way to transport it, either directly to the target (e.g., a port) or indirectly by landing it in Mexico, Canada, or the Caribbean and then moving it across a remote section of the U.S. border. Indeed, logic suggests, and most experts believe, that a port is more likely to be attacked from land than from sea, especially given the lack of visibility into the domestic trade network, the lack of protection on the landward side, and the ease of constructing explosive devices with domestic resources. Terrorists would likely construct smaller items (e.g., biological agents) domestically and then deliver them through FedEx or a similar carrier. While nuclear smuggling is possible, so are dozens of other attack scenarios. Overinvesting in countering one tactic when terrorists could easily employ another is dangerously myopic. Spending billions of dollars and deploying thousands of personnel to screen every container is an extremely inefficient and expensive way to stop terrorists from using cargo containers, especially since they would probably use other means. Choosing to screen every cargo container creates an easily bypassed bottleneck that gives people a false sense of security. Furthermore, even if these were good ideas, much of the technology, especially with regard to seals, is fairly immature. Admittedly, the Senate legislation asks for only three test sites, but why waste money on testing a bad idea?

#### Spending on container security fails.

Kochems, 05. (Alane Kochem, Policy Analyst for National Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation, Taking a Global Approach to Maritime Security, Heritage Foundation, http://www.heritage.org/research/reports/2005/09/taking-a-global-approach-to-maritime-security)

Some security analysts argue that container security should receive special consideration because a container could possibly be used to smuggle a nuclear weapon into the country. To counter this threat, they propose spending billions of dollars on container and port security.

This argument fails on four counts. First, the nuke-in-box is an unlikely terrorist tactic. If an enemy wanted to smuggle a bomb into the United States, a private watercraft would be a safer and more secure way to transport the weapon, either directly to the target (e.g., a port) or indirectly by landing it in Mexico and then driving it across the border. Second, while nuclear smuggling is possible, so are dozens of other attack scenarios. It is dangerously myopic to overinvest in countering one tactic when the terrorists could easily employ another tactic. Third, searching every container and hardening every port is extremely inefficient and expensive way to stop terrorists from using cargo containers. Fourth, there is no viable busi­ness case for many of the proposed solutions for "hardening" shipping containers. These measures would provide only minimal utility at the cost of billions of dollars in new duties or taxes.

### AT: Terrorism – Economy Impact

#### No Guarantees Against Terror Attacks; Focus on Recovery Should Be Primary

**PPIC, ‘6** (Public Policy Institute of CA, “Protecting The Ports: Are U.S. Security Measures Missing The Boat?” PPIC, <http://www.ppic.org/main/pressrelease.asp?p=631>)

SAN FRANCISCO, California, June 27, 2006 — A new study of U.S. seaport security delivers a message that leaders and citizens may not want to hear: Because there is no foolproof way to protect America’s ports from a terrorist attack, current policies and programs need to focus much more on recovery and economic restoration. In a report released today by the Public Policy Institute of California (PPIC), a team of economists and maritime security experts looks at an array of security issues to provide one of the most comprehensive examinations of port security to date. Given that 41 percent of U.S. international trade passes through the nation’s 361 seaports and that millions of American paychecks depend on this flow, how devastating would an attack be to the nation’s economy? The report’s chapters provide a range of estimates: At the high end, some of the authors argue that an attack on a major seaport such as Los Angeles-Long Beach could cost the nation tens of billions of dollars. However – if response and recovery is appropriate and sufficient – other authors find that the economic cost would be relatively small. “No matter what we do to protect the ports, it will not be enough to ensure – absolutely – against an attack at some location,” says PPIC program director Jon Haveman, who edited the volume with PPIC research fellow Howard Shatz. One of the report’s strongest recommendations is that comprehensive recovery plans be created specifically to reduce economic panic and to restore global supply chains quickly following a catastrophe. “How well government reacts to the problems caused by an attack is probably as important as how well it anticipates them,” adds Shatz. In fact, the authors also suggest that rigorous recovery plans can serve as a disincentive to terrorists, who have been shown to focus on targets where they can do the most damage—economic and otherwise.

### Solvency Answers

#### Giving ports grants does not help national security

Carafano, ‘5 (James Jay Carafano, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies and Director, Douglas and Sarah Allison Center for Foreign Policy Studies, “Homeland Security Dollars and Sense #2: Misplaced Maritime Priorities”, Heritage foundation, http://www.heritage.org/research/reports/2005/02/homeland-security-dollars-and-sense-2-misplaced-maritime-priorities?renderforprint=1)

Appropriators must ensure that funding is directed toward programs that provide the greatest contribution to the most critical missions in homeland security. Getting the "biggest bang for the buck" is a worthwhile criterion to guide these spending decisions. Nowhere is this more important than in the area of maritime security. Maritime commerce is essential to America's economic vitality. Most goods that enter and leave our shores travel by sea. But this economic lifeline also offers terrorists vast opportunities to exploit or attack ships, ports, and waterways. Nowhere should the need for strategic spending be more apparent. Yet, nowhere is it more apparent that Congress has failed to target spending where it could provide the most security. Owners and operators of **the nation's more than 350 ports have made shrill demands for increased federal grants in support of port security**. Indeed, **estimates for enhancing security at America's ports run into the billions of dollars**. The Administration proposed limiting port grants in FY 2005 to $50 million. Lobbying efforts pushed for dramatic increases-as much as $400 million per year. In the end, Congress settled on tripling funding to $150 million. Is that a victory for enhancing maritime security? Not at all. The Administration was prudent to ask for more limited spending. **The U.S. port infrastructure is so vast that providing resources for other than the most critical needs makes little sense. Spreading $150 million across the nation won't come close to plugging all the security gaps at ports. It is akin to locking the door in a house without windows**. On the other hand, grant programs have proven far more effective when federal money has been used to fund vulnerability assessments and to encourage public-private partnerships that adopt sustainable and effective port-security programs. T**o address the considerable vulnerabilities of maritime infrastructure, the greater**

**share of federal dollars might be more effectively used to invest in effective intelligence and early warning, domestic counterterrorism, and border and transportation security programs-efforts that would keep terrorists out of the ports to begin with**. Congress should ensure that Coast Guard modernization is fully funded before it even thinks about dumping more federal dollars into port grants **for state, local, and private sector projects that contribute marginally to the overall security of the maritime domain. The Administration and Congress should refrain from increasing port security grants** in the FY 2006 budget

#### Current tech incredibly expensive and ineffective

Carafano and Zuckerman, 12 (James Jay Carafano and Jessica Zuckerman, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies and Director, Douglas and Sarah Allison Center for Foreign Policy Studies and Research Associate, Douglas and Sarah Allison Center for Foreign Policy Studies, “Maritime Cargo Scanning Folly: Bad for the Economy, Wrong for Security”, Heritage foundation, <http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate>)

Cost and infrastructure are also important factors. A single x-ray scanner, the most common technology used for cargo screening, can have a price tag of $4.5 million, plus an estimated annual operating cost of $200,000, not to mention the roughly $600,000 per year for the personnel required to run the equipment and examine the results.[3]

Likewise, the mere placement of scanners can also prove to cause logistical problems, as many ports were not built with natural bottlenecks through which all cargo passes. With today’s economy relying heavily on the timely and efficient

movement of goods, and such logistical delays could amount to around $500 billion in total profit loss. And once scanning technology is installed, it may encounter multiple problems, such as incompatibility with previous technologies, frequent outages due to weather, and insufficient communication infrastructure to transmit electronic data to the U.S. National Targeting Center-Cargo, where it is assessed.

#### No amount of money will make Port security safe

Wolf, 09/13/2006[Bryon Wolf, Political Editor and Deputy Political Director for abc news , ÔøΩHow much is too much for Port Security?,ÔøΩ world news, <http://abcnews.go.com/US/Politics/story?id=2425748&page=1#.T-Hnc47wefQ>]

Homeland Security Secretary Michael Chertoff also asked a Senate panel to weigh how much safety the country could afford. **Despite billions of dollars already spent**, he argued, the **government can't ensure 100 percent safety.Chertoff** probably didn't expect to find himself **drawing** the **analogy between car accidents and port security**, but that's what he did in one awkward exchange.He said to the panel that **no matter how careful drivers were, people were going to die in car crashes**.Then he implied the **same** was **true of port security**, suggesting there was **no way to entirely safeguard AmericaÔøΩs ports.**

#### Spending on container security fails.

Kochems, 05. (Alane Kochem, Policy Analyst for National Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation, Taking a Global Approach to Maritime Security, Heritage Foundation, http://www.heritage.org/research/reports/2005/09/taking-a-global-approach-to-maritime-security)

Some security analysts argue that container security should receive special consideration because a container could possibly be used to smuggle a nuclear weapon into the country. To counter this threat, they propose spending billions of dollars on container and port security.

This argument fails on four counts. First, the nuke-in-box is an unlikely terrorist tactic. If an enemy wanted to smuggle a bomb into the United States, a private watercraft would be a safer and more secure way to transport the weapon, either directly to the target (e.g., a port) or indirectly by landing it in Mexico and then driving it across the border. Second, while nuclear smuggling is possible, so are dozens of other attack scenarios. It is dangerously myopic to overinvest in countering one tactic when the terrorists could easily employ another tactic. Third, searching every container and hardening every port is extremely inefficient and expensive way to stop terrorists from using cargo containers. Fourth, there is no viable busi­ness case for many of the proposed solutions for "hardening" shipping containers. These measures would provide only minimal utility at the cost of billions of dollars in new duties or taxes.

### Solvency Answer – Forgery

#### Can’t solve port security – too easy to forge

Waterman 11 (Shaun Waterman, award winning reporter for the Washington Times, senior editor and correspondent for United Press International for nearly a decade, covered Department of Homeland Security since 2003, earned “Dateline Washington” award from Society of Professional Journalists; “Ports vulnerable to gaps in access-ID system; Cards forged, obtained illegally; biometric data unread” The Washington Times, Lexis Nexis) <http://www.lexisnexis.com/lnacui2api/auth/checkbrowser.do?rand=0.9439895296448221&cookieState=0&ipcounter=1&bhcp=1>

Special identification cards used by maritime workers to protect the nation's ports from terrorist infiltration can be forged or fraudulently obtained with relative ease, according to congressional investigators. Undercover investigators covertly tested the security of the ID cards used for access to ports around the country and found "significant weaknesses" in the security of the program, stated Stephen M. Lord, director of homeland security and justice issues for the Government Accountability Office, in prepared testimony before the Senate Commerce, Science and Transportation Committee. A copy of his testimony was obtained by The Washington Times.

### Solvency Answer – Nuclear Material Detection Fails

#### Efforts to prevent will fail, no solvency

de Rugy November 2007 (Veronique de Rugy; Veronique de Rugy is a senior research fellow at the Mercatus Center at George Mason University. de Rugy directed academic programs in France for the Institute for Humane Studies-Europe. Dr. de Rugy received her MA in economics from the University of Paris IX-Dauphine and her PhD in economics from the University of Paris.; “Is port security funding making us safer?”, Audit of the Conventional Wisdom, MIT, http://web.mit.edu/cis/pdf/Audit\_11\_07\_derugy.pdf)

In addition, the Department of Homeland Security (DHS) spent $60 million on the Custom and Trade Partnership against Terrorism (C-TPAT). The 7,000 businesses, including most of the largest U.S. importers, involved in this public-private and international partnership have agreed to meet “supply chain” standards for establishing a secure chain of custody for every unit of cargo traded overseas. Sadly, recent reports have found crippling flaws in DHS’s foreign programs. The Domestic Nuclear Detection Office (DNDO) received $535 million in 2007. DNDO’s mission addresses a broad spectrum of radiological and nuclear protective measures, but is focused exclusively on domestic nuclear detection. The fundamental problem is that DNDO relies on radiation portal monitors that have been proven unable to detect shielded nuclear material essentially rendering them useless.

### Solvency Answer – Tech Insufficient

#### Technology doesn’t solve

Keefer, J.D, 2008 (Wendy J. “Container Port Security: A Layered Defense Strategy to Protect The Homeland and The International Supply Chain” Campbell Law Review Vol. 30:139)

Ultimately, some of the success in this arena will depend upon advancements in technologies that can be made available at reasonable prices. Security technology is continuously evolving, not only in terms of capability but also in terms of compatibility, standardization, and integration with information systems. It is important to note that there is no single technology solution to improving supply chain security. As technology matures, it must be evaluated and adjustments to operational plans must be made. Priority should be given to effective security solutions that complement and improve the business processes already in place, and which build a foundation for 21st century global trade. A more secure supply chain also can be a more efficient supply chain.

### RFIDs Fail

#### RFID systems are limited – too many tech problems

Englert et al 2007 (Burkhard Englert, Dolgorsuren Byambajav and Aniketh Parmar, Department of Computer Engineering and Computer Science California State University Long Beach, “Evaluating and improving the security of RFID tags in eSeals

at the L.A. and L.B. Ports,” METRANS Transportation Center, <http://www.metrans.org/nuf/2007/documents/EnglertRFIDpaper.pdf>)

5 Recommendations So far RFID Systems are only used in a very limited fashion at the ports of L.A. and L.B. (e.g. Pierpass). In the case of eSeals not much progress has yet been made at the ports of Los Angeles and Long Beach. While other ports and supply chains are currently in the process of testing such applications (Hong Kong to Japan, Shanghai to Savannah, the Port of Busan South Korea etc.), progress has been relatively slow at the L.A. and L.B. ports. There are several possible reasons for this delay. 1. Besides all the promises made by RFID System manufacturers the technology has not yet matured sufficiently. There are still many unresolved issues with respect to reliability. The failure rate of many RFID systems is still too high causing many companies to hesitate with an investment. 2. Many interoperability problems have not yet been addressed. It still appears to be very cumbersome to integrate an RFID system with existing enterprise software. Many companies simply do not want to invest into new technology that they cannot seamlessly integrate into their existing systems. 3. Until recently there was a complete lack of eSeal communication standards. 4. There is still widespread concern about the security of eSeals. 5. These issues combined lead to the general perception of a non existent or very low return on investment in an eSeal RFID system, re-enforcing many a®ected companies in their "wait and see" attitude.

#### Security Problems with RFID abundant

Englert et al 2007 (Burkhard Englert, Dolgorsuren Byambajav and Aniketh Parmar, Department of Computer Engineering and Computer Science California State University Long Beach, “Evaluating and improving the security of RFID tags in eSeals

at the L.A. and L.B. Ports,” METRANS Transportation Center, <http://www.metrans.org/nuf/2007/documents/EnglertRFIDpaper.pdf>)

3 RFID Security We will now discuss some of the main possible security problems associated with RFID Systems. 3.1 RFID Risks and Threats 1. Privacy Attacks. One of the most fundamental problems associated with RFID tags that still needs to be addressed is privacy, that is items that are tagged indiscriminately reveal sensitive information when queried by a reader. This may also lead to tracking, a violation of location privacy. Since most tags when queried always provide the same identifier it is possible to establish an association between a tag and its owner. Even in cases where tags do not reveal any valuable information that could be used to identify them it might still be possible using an assembly of tags to perform this kind of tracking. 2. Physical attacks. In this case tags are manipulated physically, e.g. radiation imprinting, circuit disruption, clock glitching. Tags usually are not resilient against such attacks. 3. Counterfeiting. In this case tags are directly manipulated to modify the identity of an item. 4. Spoofing. In a spoofing attack an attacker successfully impersonates a legitimate tag. The attacker can, for example, record the signal transmissions between tag and reader (if the attacker is close enough to both tag and reader) and replay them when desired to impersonate the recorded tag. 5. Eavesdropping. In this case attackers are able to intercept and read RFID communications. 6. Skimming Attacks. Most RFID devices today broadcast a static identifier without any explicit authentication procedure. As a result an attacker in a so called skimming attack can simply scan identifying data. Such skimmed data can then be used to produce cloned tags, exposing several lines of attack. In the case of shipping containers for example, an attacker could feasibly break into a container and then replace the now silent tag with a cloned tag that simply rebroadcasts the id skimmed from the original tag. Such a container would then most likely escape inspection. Another possibility would be that in a swapping attack the attacker simply swaps the original container and its RFID tag with an alternate container and its cloned tag. 7. Denial of Service, e.g. signal jamming of RF channels. Clones can also create denial of-service issues. If several, valid-looking clones appear simultaneously at a port, should they be honored as legitimate? Or must they all be inspected and rejected as fraud? In this way cloned tags could be intentionally designed to corrupt supply chain databases. Recently researchers were able to demonstrate practical cloning attacks against real world RFID devices. Mandel, Roach and Winstein (Mandel et al. 2004) showed how to read access control proximity card data from a range of several feet and produce low cost clones. This was possible even though the cards they tested themselves had a legitimate read range of only several inches. Researchers from Johns Hopkins University and RSA Laboratories (Bono et al. 2005) recently studied and performed attacks against cryptographically enabled RFID tags as they are used in payment and automobile immobilization systems. In their attack they were able to extract secret keys using reverse engineering and to simulate target transponders. They showed an existing risk of auto theft from the compromise of RFID systems. 8. Traffic analysis. In this case an attacker attempts to extract information from a pattern of communication. Such an attack is possible even if the messages transmitted are encrypted. 5

#### RFIDs fail in a number of ways

Ma, 2011 (Di Ma, Security And Forensics research Laboratory SAFE Lab, Department of Computer and Information Science, University of Michigan-Dearborn, “A Context-Aware Approach for Enhanced Security and Privacy in RFID Electronic Toll Collection Systems”, Univ. of Michigan-Dearborn/Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference, http://ieeexplore.ieee.org/xpls/abs\_all.jsp?arnumber=6006281)

RFID Electronic Toll Collection (ETC) systems have been deployed worldwide to improve toll collection efficiency, reduce road congestion, increase road safety and traveler satisfiability. However, the use of such systems raises a number of security and privacy issues due to unauthorized reading and relay attacks. Unfortunately, currently deployed or proposed solutions targeting these attacks often fail to satisfy the constraints and requirements of the underlying RFID toll road application in terms of (one or more of) efficiency, security, and usability. In this paper, we report our initial work toward a new approach, one that utilizes sensing technologies, to tackle the problems of unauthorized reading and relay attacks in RFID ETC systems by considering efficiency, security, and usability simultaneously. In our approach, on-board tag sensors are used to collect contextual information (location, speed) about the tag. Such contextual information is then used to design context-aware selective unlocking mechanisms for toll cards such that they can selectively respond to reader interrogations and thus minimize the likelihood of unauthorized reading and relay attacks. The premise of our work is a current technological advancement that enables many RFID tags with sensing capabilities.

#### Reliability and Cost are major issues with RFID Technology

Haveman and Shatz, 2006 (Jon D. Haveman and Howard J. Shatz, Editors at the Public Policy Institute of California; Library of Congress, “Protecting the Nation’s Seaports: Balancing Security,” Public Policy Institute of California, <http://www.ppic.org/content/pubs/report/r_606jhr.pdf>)

In-Box. “Sniffers”—in-box sensors—to detect radiation, people, light, motion, temperature, humidity, explosives, specific chemical traces, etc., constitute another distinctive layer of defense. They figure prominently in most proposals for getting serious about container security, as well as in the Department of Homeland Security’s ambitions to significantly improve port security. U.S. Customs and Border Protection Commissioner Bonner announced that the department is eager to quickly adopt in-box sensors and radio frequency identification (RFID) technology for container tracking. The sensors, placed securely inside the container, should be able to operate all the time or, if that poses a difficulty (perhaps because of limited battery power), switch on and off frequently, taking real time readings and relaying them via radio frequency or some alternate communications technology to U.S. authorities. Location tracking as well as detection is integral to almost every proposal. (Indeed, tamperproof locks and location trackers invariably come first on every list; they are far cheaper than sensors, are already proven, and carry a positive commercial benefit. They show if the container has been opened and where it is; unfortunately, they do not detect weapons or improper cargo.) The sensors would operate from the time of loading all the way through the point of unloading. Reliability is a critical concern: False positives would bring down the international trade system or else could make the sensors into something like car alarms in a city, angering and ignored. Commissioner Bonner, aware of this problem, sets the date for rapid adoption for “as soon as the technology to reduce false positives to an acceptable level is there to do so, and not a day later.” Cost is another consideration. There may be a very limited number of high-volume container ports in the United States, but there are about 15 million containers in circulation worldwide. Even with a resulting selection of containers suitable for shipment into the United States, that would still leave several million to equip. The cost of active detector systems as discussed above for in-port use, barring a thousand-fold fall in their price, is simply out of the question: Millions of containers at a million dollars each yields federal budget size numbers. In-box means, therefore, passive. But because findings are transmitted to the next lines of defense, false positives need not result in the delays and costs associated with in-port false positives. Cost estimates for equipping containers differ considerably. The cost for tamper-proof locks and location trackers is low. The most common number that includes sensors, and not just locks and RFID, is $500. This amount nicely generates estimates of commercial benefits such as the $1,200 per container by one vendor, Savi Technology. But doubling that cost to $1,000 seems prudent while still remaining useful for our purposes. The initial total cost number seems a bit shocking: $15 billion dollars to equip the container fleet.

#### RFIDs empirically fail and are inefficient – Long Beach Port proves

Homeland Security News Wire February 20 2009 (The Homeland Security News Wire is a leading e-information service, delivering daily digital reports, in-depth analysis, news, and researched background on the day’s developments in homeland security, “Big problems with RFID deployment at Los Angeles – Long Beach ports,” <http://www.homelandsecuritynewswire.com/big-problems-rfid-deployment-los-angeles-long-beach-ports>)

The first day of using RFID tags caused a reported 1,500 trucks to be turned away from the Port of Los Angeles and delays of more than an hour at the Port of Long Beach This is the story of progress: two steps forward, one step back. Here is an example: RFID tag problems caused jams at Los Angeles, Long Beach ports. The first day of using RFID tags caused a reported 1,500 trucks to be turned away from the Port of Los Angeles and delays of more than an hour at the Port of Long Beach. The mega ports -– which, during prosperous times, claimed to import 40 percent of the U.S. goods -– approved Clean Truck Programs this past fall that banned pre-1989 diesel engine trucks. The Clean Truck Programs will ban pre-1994 trucks on 1 January 2010. By January 2012 all diesel trucks with engines 2006 and older will be banned. The ports began charging $35 per 20-foot container unit on Wednesday, 18 February, and used RFID to control the access. In some cases, the RFID did not work, and many long traffic jams resulted, several newspapers reported. According to the Daily Breeze, an estimated 15 percent of drivers were denied access from the ports because of not having the Clean Truck Plan-required RFID chips. The Port of Long Beach, ironically, has scheduled a special Harbor Commission meeting for Monday to consider lowering some container fees in an effort to increase port traffic, which is down about 25 percent from a year ago.

#### RFIDs fails – international inconsistency and expenses

Giermanski ‘05 (James Giermanski. Director for the Center for Global Commerce, Belmont Abbey College. “RFID is Not the One.” Cargo Security International. http://www.gatekeeperusainc.com/industry-news/rfid-is-not-the-one.html)

It seems that RFID – the short term used to refer to radio frequency identification – has become the current ‘buzz word’ among some of the largest retailers and importers in the United States. Wal-Mart and Target are just two of the giants discussed in the literature. Recently, an A. T. Kearney report entitled Smart Boxes lauded the potential and actual use of RFID for certain supply chain applications.

However, the application of RFID to container security and port security is less laudable, less effective, more costly, and certainly questionable as a primary means of international transportation security for containers. RFID applications, whether active or passive, have very clear weaknesses and impediments to usage in a world-wide context. The impediments are these: the absence of agreement on RFID world-wide standards; its land-based character; and the rights to acquisition, cost, and control of required RFID infrastructure. Protocols and standards. RFID applications require the carriage and transmission of data through a wireless system. Data can be loaded into a device called a transponder, and can then be transmitted via radio waves when the transponder is triggered by a corresponding device called a transceiver or reader. The transponder is a slave RFID unit that reacts to a triggering radio frequency message from the master transceiver. The transceiver, through its antenna, sends the triggering frequency, which produces a return transmission of the data pre-loaded into the transponder like manifest or shipping data or information acquired by the RFID device like the opening of the container door. Since the transmission of these data is by electromagnetic waves, the successful transmission is subject to the use of the proper frequencies or waves and the absence of distortion like noise or same-frequency emissions from competing antennas whose direction (footprint) unintentionally or intentionally obstructs or interferes with the intended RFID transmissions of the intended transponder. In order for the transponder and reader to talk to each other, they need to speak in the same way. In other words, they must follow a protocol or a set of instructions. While no analogy is perfect, assume it is something like one person speaking Spanish and the other English and at different speeds, with different volumes, and both talking at the same time. In our analogy, protocols tell each person (in the real world, the container and the reader) when to start and stop, what language to use, how fast to talk etc. Unless the instructions are clear to each, communication may not take place. There are no global protocols or standards, however. Imagine the lack of standardized instructions for a container and its transponder on a global voyage: different regions will have different standards. There are national standards like those from the American National Standards Institute (ANSI), international standards from the International Organization for Standardization (ISO), and industrial standards like the Electronic Product Code (EPC) from EPCglobal Inc. ISO has 12 standards related to RFID. In other words, until there is some universal or global protocol or set of instructions, RFID usage on shipping container security is unlikely. Frequencies, too, have different bands, like low, intermediate, and high. Each band is more appropriate for unique usage. For instance, low-frequency RFID is used for short to medium distances, low speed, and simple applications such as access controls. Intermediate frequency bands can also be used for access control also but offer a little faster read speed. High-frequency RFID is used for fast read speeds and if the specific standard allows high wattage output, longer range can be obtained. The major problem is the frequency approved for use by different governments. Like protocols, RFID approved frequencies differ globally. Thus, RFID on which the data ride in the United States will not work in another part of the world. The foreign transceiver cannot trigger the data transmission because the US may use a different frequency. For example, the United States Federal Communications Commission (FCC) issued a final rule effective on 23 June 2004 that only 433 MHz RFID systems can be used for commercial shipping containers. Likewise, other countries in other RFID frequency regions have approved different frequencies for different uses. Therefore, RFID for container security is applicable only to those areas of the world which have agreed on the same frequency for the same usage, precluding a standardized global use of RFID for shipping containers. Land-based character. In addition to the frequency problem exemplified by a lack of world-wide standardisation, an equally troublesome area for RFID usage in container security is the overland movement of containers and the corresponding creation of a landbased infrastructure of antennas and readers. Unlike RFID tags used in products and pallets which are read in controlled distribution systems, active RFID devices in containers which move around the world through uncontrolled environments require the construction of antennas at chokepoints (those points along the journey of the container which cannot be circumvented by the carrier). Constructing a controlled distribution path globally is really impossible. The A.T. Kearney report defines chokepoint location this way: ‘Chokepoints where readers might be positioned include the spot where a truck is loaded or unloaded, on a crane that transfers containers, a weigh station, the port of loading, or at the port of discharge.’ Only for these obvious chokepoints, at origin and destination, is a land-based system a reasonable option.

#### Multiple problems with RFIDs

Piramuthu, 27 January 2007 (Selwyn Piramuthu, American Economic Institutions Professor, Full Professor, PHD - Information Systems, University of Illinois MS, University of Arizona, BS, Indian Institute of Technology, Madras, India, “Protocols for RFID tag/reader authentication,” http://www.sciencedirect.com/science/article/pii/S0167923607000103)

Radio-Frequency Identification (RFID) refers to technologies and systems that use radio waves (wireless) to transmit and uniquely identify objects [14] and [21]. It generally involves an RFID transponder or tag, which comprises a chip and an antenna that are together attached to an object that is to be identified and/or tracked. The antenna allows the chip to transmit stored information about the object of interest to a reader. These chips can store about 2 kb of data. Tag readers are used to retrieve data stored in RFID tags. Antennas are used to send and receive radio waves and signals between tag readers and RFID tags. The tag reader is connected to a back-end server and database for relatively heavy-duty processing (e.g., authenticating a tag using an identifier that is embedded in a keyed hash function).

RFIDs were first used in WW-II as IFF (Identify Friend or Foe system). Although RFID technology is decades old, there has been renewed interest in utilizing its beneficial properties from researchers and practitioners alike. RFID technology is used to facilitate information sharing in decentralized business environments such as supply chains [18]. Based just on WalMart's mandate and that of U.S. Department of Defense (US-DOD), the RFID tag market in the U.S. retail supply chain was $91.5 million in 2003, and is expected to be around $1.3 billion in 2008 (U.S. RFID for the Retail Supply Chain Spending Forecast and Analysis, 2003–2008, IDC.com, 2005). The value of total market, including systems and services, is projected to be around $26.9 billion in 2015 [20]. Gartner [15] estimates the market for RFID tags to be around $3 billion in 2010.

Privacy and security issues play a major role in the success of RFID tag implementations due to the ease with which the object they are attached to can be identified and/or tracked by an adversary. Most existing implementations of RFID tags are not secure, and can leak data about the object to which they are attached. An adversary can also silently track/monitor the object. Some common types of attacks on RFID tags include eavesdropping, replay attack, man-in-the-middle attack, loss of data including DoS (denial of service) and message hijacking, skimming and forgery (including cloning), and physical attack. The reader is referred to Avoine and Oechslin [2] for detailed description of these and other types of attack on RFID tag/reader. Although there are means to protect tags against some of these attacks, newer vulnerabilities are discovered often enough that there seems to be no such thing as perfect protection (e.g., [6] show how they defeated the security of an RFID device known as a Digital Signature Transponder manufactured by Texas Instruments that helps secure millions of highway toll payment transponders and automobile ignition keys; [33] present details of virus attack on RFID tags; SCISSEC [36] present a DoS attack against Frequency Hopping Spread Spectrum). For excellent surveys on security/privacy issues as related to RFID tags, the reader is referred to Garfinkel et al. [42] and Rieback et al. [34].

Privacy and security issues play critical role in acceptance of RFID tags by the general public since most people are circumspect of being monitored/tracked/watched/etc. (see, for example, www.rfidkills.com, www.stoprfid.org, www.spy.org.uk/cgi-bin/rfid.pl). Although other means of tracking people (e.g., video surveillance) are already in widespread use, some of the inherent properties of RFID tags renders opportunities for suspicion including their low cost, physical size, extended lifespan when battery power is not used, extensive data generation capability, and the absence of an off switch.

There exist a few means to disable tags from being read. For example, the Blocker tag presented in Juels et al. [27], Clipped tags presented in Karjoth and Moskowitz [28], metal or foil-lined containers (e.g., wallets) that are impenetrable to radio-frequency waves (Faraday cage), and the case where the user simply destroys the tag along with the tagged object [39]. Castelluccia and Avoine [9] propose ‘noisy’ tags to confuse an adversary from deciphering reader/tag conversation. Although these are important issues, we are interested only in the technical aspects of RFID security/privacy. Given the cost, limited storage and computational capacity of these tags, resource allocation addressing security/privacy concerns invariably are insufficient. Market forces dictate lower cost with more usable functionality, whereas security/privacy issues generally do not improve bottom lines. Even if the entire set of resources available on an RFID tag are used for cryptographic protocols, standard cryptographic algorithms (e.g., RSA) cannot be used to support authentication protocols in passive RFID tags due to their storage and processing limitations. For example, even the higher-end passive tags have at most 2000 gates for security purposes while a standard cryptographic algorithm would require gates in the order of tens of thousands [26]. Moreover, storage requirements for these algorithms prove to be insufficient as well. Moore's Law is not a consolation here due to market price pressures [26].

When dealing with privacy/security issues in passive RFID tag implementations, their processing power and memory constraints therefore dictate lightweight authentication protocols. Several researchers have proposed and evaluated protocols that fit the bill of being lightweight and at the same time being secure to a reasonable extent [2], [13] and [40].

Over the past few years, several streams of research have emerged that deal with authenticating tags and tag readers. We consider a few such streams of research and their resulting authentication protocols. Specifically, we consider the following: single round protocols for single tag, multiple round protocols for single tag, single round protocols for multiple tags, and protection against relay attacks. These protocols, by their very nature, tend to be heuristic-based or are sometimes based on reduction to NP-hard problems.

The contribution of this paper are three-fold: we present an overview of various streams of research involving RFID tag/reader authentication; we present privacy/security vulnerabilities in existing protocols identified by other researchers as well as new ones; we propose modifications to existing vulnerable protocols without proof.

This paper is organized as follows: the next section provides an overview of several single round protocols for single tag. Section 3 presents an overview of several multiple round protocols for single tag. Section 4 presents an overview of single round protocols for multiple tags. Section 5 presents an overview of relay attacks. The final section concludes the paper with discussion of overview as well as modifications presented in this paper.

### RFIDs Bad – Bomb Detonator

#### RFIDs can be used as triggers for bombs

Kimery ’11 (Anthony Kimery. Online Editor and Online Media Division manager of Homeland Security Today. “RFID Signals Can Detonate Bombs In Cargo Containers: But How Serious Is The Vulnerability)

In the fall of 2007, a handful of officials from the Department of Homeland Security (DHS) were invited to attend a live demonstration of how a bomb hidden inside a commercial cargo container could be detonated by a homemade radio frequency identification (RFID) container tracking tag operating at a frequency that was mandated by the federal government for cargo containers within US port environments. A cargo container RFID electronic tag, or seal, contains an electronic reader that receives a port’s RFID signal that prompts the container’s RFID tag to transmit to port authorities data regarding the cargo that’s been encoded on its RFID tag. But as the demonstration showed, it also can be used to close an electronic circuit when it receives a corresponding RF from a port RFID sender/receiver, thereby detonating the bomb. Indeed. In the November, 2007 test, an RF receiver tuned to pick up a required US port RFID reader frequency triggered the small explosive that had been placed inside the empty container. None of the DHS officials though – including officials from Customs and Border Protection (CBP) - who were invited to attend the demonstration showed up. Had they been present, they would have witnessed the homemade RF receiver – which had been assembled by a college student using about $30 worth of easily obtainable parts and programmed to operate at a frequency cargo container RFID tracking tags are required to utilize – successfully be used to trigger the detonation of the explosive in the container.

## \*\*\*Offcase\*\*\*

### Federalism Link

#### Port management is a states right.

Keefer, J.D, 2008 (Wendy J. “Container Port Security: A Layered Defense Strategy to Protect The Homeland and The International Supply Chain” Campbell Law Review Vol. 30:139)

The United States is served by more than 360 commercial ports that provide approximately 3,200 cargo and passenger handling facilities, according to the U.S. Coast Guard. Depending on the individual port facilities, they may accommodate anything from recreational watercraft, to barges, ferries, and ocean-going cargo and passenger ships. Governance of these ports in the United States is a function of various state and local public entities, such as port authorities, port navigation districts and municipal port departments. Currently, there are more than 160 cargo- and passenger-handling ports under the jurisdiction of 126 public seaport agencies located along the Atlantic, Pacific, Gulf and Great Lakes coasts, as well as in Alaska, Hawaii, Puerto Rico, Guam, and the U.S. Virgin Islands. Many of these seaport agencies are governed by an elected and/or appointed body, such as a port commission. 28

### Multilateral Code of Conduct CP

#### Text: The United States Federal Government should hold an international conference to propose the creation of an international Code of Conduct for the purpose of improving shipping container security.

Or

#### Text: The European Union should hold an international conference to propose the creation of an international Code of Conduct for the purpose of improving shipping container security.

#### This gets other countries on board for multilateral action

Dahlman et al, OD Science Applications, Sweden, 5

(Ola, Jenifer Mackby, Bernard Sitt, Andre Poucet, Arend Meerburg,

Bernard Massinon, Edward Ifft, Masahiko Asada, Ralph Alewine

“Container Security: Proposal for a Comprehensive Code of Conduct,”

Defense & Technology Papers are published by the National Defense University Center for Technology, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434718)

The most urgent next step is to explore and mobilize the political will to negotiate a Code of Conduct on Container Security and identifying a proper forum for such negotiations. Consideration of container security is taking place in individual states (in particular the United States), in international fora such as the EU and OSCE, as well as organizations such as the IMO and WCO and among industries.

The negotiations of a Code of Conduct envidsioned here would best be held among States in a worldwide forum with the participation of international organizations and industry. As there is no natural entity that has the mandate to take such an initiative, there is a need for an individual actor to initiate the process. Negotiations might be conducted within the framework of the IMO or the WCO, for example, though neither has the full responsibility for the entire transport chain. Alternatively, one country could take the initiative to call for an international conference to develop a Code of Conduct; the creation of the Ottawa Treaty banning anti-personnel landmines is an example of such a negotiation among the willing.

The EU or the OSCE might be able to agree on a regional Code of Conduct that could be expanded globally. Another possibility would be that the G8 plus China initiate the development of a code during their summit meeting in 2005 by creating a negotiating process. The expanding economy of China and the importance of Hong Kong in the world container trade would be an incentive for China to join such a negotiation as a follow up to the G8 Summit Agreement in Kananaskis of 2002, where the G8 agreed to develop pilot projects to model an integrated container security regime.

\*WCO – World Customs Organization

\*\*IMO – International Maritime Organization

#### A multilateral Code of Conduct for maritime trade solves container security

Dahlman et al, OD Science Applications, Sweden, 5

(Ola, Jenifer Mackby, Bernard Sitt, Andre Poucet, Arend Meerburg,

Bernard Massinon, Edward Ifft, Masahiko Asada, Ralph Alewine

“Container Security: Proposal for a Comprehensive Code of Conduct,”

Defense & Technology Papers are published by the National Defense University Center for Technology, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434718)

Container security is not just a national issue for a single country, but rather an international issue and it should be implemented on a global scale for all modes of transport in order to work satisfactorily. The current initiatives discussed above, while providing a good start at improving security arrangements for container transport, do not address the end-to-end security problem. There is no over-arching framework to address the container security problem that builds on the current bifurcated approaches of treating the customs and transportation elements separately. A government-sanctioned, multilateral regime is needed to provide security accountability standards for all elements of container operations. Such an approach could lead to a harmonization of security requirements that can be applied to the container transportation operations from beginning to end: importers/exporters, port authorities, and shipping industry.

Within such a framework, it would be possible to formulate a market-based set of incentives that would be driven by an enhanced security regulated environment. Realization of a Code of Conduct requires a strong push from governments and the active participation of industry. A multilateral Code of Conduct should make it possible to obtain the needed cooperation of all the stakeholders if the enhanced security is seen as “leveling the playing field” and if there were strong economic incentives for industry. Strong continuing oversight of the security regime is also required.

It should be noted that there is currently no forum in which governments, industry and international organizations can discuss the development of a more encompassing Code of Conduct. Identification of such a forum should be a priority to develop the details of a Code of Conduct. In the light of its increased engagement in transport security, the WCO might be the proper forum to bring all the transport stakeholders together and facilitate an international agreement on Container Security.

We have previously identified a number of factors that contribute to the risks in container transport, such as:

• Almost 50 million containers capable of carrying large, heavy loads of materials, including high explosives and WMD that could be used for terrorist activities, are routinely transported around the world and a single one could pose a deadly threat;

• Only two percent of all containers that pass through a harbor or any other transport hub are inspected;

• The basic transport document, the bill of lading, describing the content of the container is rarely verified;

• The transport chain is not fully transparent and it involves a number of actors, many of whom are business companies;

• No authority or industry is fully responsible for the security of the entire transport chain from sender to receiver, although national customs services are fully involved;

• Although the transport history of the container might be known to a large shipping company, there are no established procedures or systems for sharing this information;

• During the initial part of transport many containers are for a long time in the custody of a single truck driver traveling large distances.

Purpose of agreement

An agreement on container security should significantly reduce the security risks in container traffic while facilitating fair and efficient global trade. As recognized by another study group that examined the container security issue, “International agreements to coordinate standards and to develop protocols for authoritative action will be essential. A suitable institution with membership that includes the majority of trading states should follow the testing programs and prepare options for such agreements.” 15

An agreement on container security could contain the following elements:

• commit States and transport actors (shipping companies, harbor authorities, etc.) to promote fair, efficient and secure global trade;

• commit States and transport actors to prevent containers from being used for illicit purposes;

• commit States to put all international container traffic under effective control;

• include strong national implementation measures that provide incentives for the transport industry to comply with the Code;

• establish an international cooperative regime that will support the authorities and industry in implementing the agreement.

International Measures

National authorities in States Parties to the agreement would be responsible for establishing secure container transport in accordance with this new agreement, with existing international commitments and with national legislation. Internationally established norms and procedures and co-operative verification measures would be designed to support the national authorities and the commercial actors.

The international measures would:

• Establish document standards and procedures for transmission and checking the authenticity of such documents using modern technology;

• Establish procedures for verifying declarations at points of origin;

• Establish standards and procedures for checking containers at harbors and at similar control posts for trains and trucks. Such standards and procedures would apply to the use of radiation detectors, thermal or x-ray imaging, swipes, and air samplers;

• Establish procedures to monitor container movements in and out of harbors, including transport history, and to make this information available to national authorities along any given transport chain;

• Establish standards for unique identification of containers;16

• Establish standards for tamper-indicating seals and a transponder system to be applied to containers;

• Establish procedures for certifying seals, transponders and equipment used for container screening and monitoring in harbors and other checkpoints;

• Assist in the national establishment of equipment and checking procedures in harbors and other checkpoints;

• Assist in the training of personnel in national authorities.

### EXT – Multilateral Code of Conduct CP

#### Implementation information

Dahlman et al, OD Science Applications, Sweden, 5

(Ola, Jenifer Mackby, Bernard Sitt, Andre Poucet, Arend Meerburg,

Bernard Massinon, Edward Ifft, Masahiko Asada, Ralph Alewine

“Container Security: Proposal for a Comprehensive Code of Conduct,”

Defense & Technology Papers are published by the National Defense University Center for Technology, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434718)

Implementing organization

Existing arms control treaties and agreements have shown that the governing and implementing organizations can be of varying sizes and can have different responsibilities. Some treaties are essentially lacking a central authority whereas others have a large implementing organization to operate verification systems, conduct on-site inspections as well as analyze, and in some cases also assess, the information collected.

An international coordinating mechanism would be required to oversee the implementation of the Code of Conduct by the Parties. The tasks of the ICM will consist of the development and review of the measures delineated above.

The international coordinating mechanism will consist of a General Conference of all States Parties meeting on a regular basis, Working Groups and a small Secretariat. Working Groups will deal with specific issues and report back to the General Conference. The Secretariat will prepare the conferences, support Working Groups and assist in the oversight of the implementation of the Code. Industries that have adopted the obligations of the code may participate as observers in the General Conference and may participate in the work of the Working Groups, as appropriate.

To implement a Code of Conduct on container security, it should be realized that international container traffic is only one--albeit important--part of international trade. It should be explored whether an existing, preferably worldwide, organization involved in international trade, such as the IMO or the WCO, could serve as the implementing organization. This would be a new mission. Maximum cost-benefit could be gained by sharing the governing body, secretariat, training facilities etc. of such an organisation.

#### Consulting the private sector is key to solve

Dahlman et al, OD Science Applications, Sweden, 5

(Ola, Jenifer Mackby, Bernard Sitt, Andre Poucet, Arend Meerburg,

Bernard Massinon, Edward Ifft, Masahiko Asada, Ralph Alewine

“Container Security: Proposal for a Comprehensive Code of Conduct,”

Defense & Technology Papers are published by the National Defense University Center for Technology, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434718)

Container traffic involves a large number of actors around the globe, including business companies, customs authorities, and international organizations such as IMO and the World Customs Organization (WCO). It is clear that shipping companies and port authorities will play a major role in implementing any new security measures. In order to gain their support for such efforts, as well as to assure that these efforts are realistic and effective, industry should be consulted and brought into the process at an early stage. As industries are concerned about new costs, delays, added responsibilities and possible inequities in competition, it would be in their self-interest to take the lead in formulating more effective procedures, rather than having them imposed by governments. An initiative by the largest operators-- for example, AP Møller, PSA Singapore, P&O Ports, and Hutchinson Hong Kong— might lead the way to a broad engagement of industry.

Different arms control agreements, such as the Chemical Weapons Convention (CWC), the Nuclear Non-Proliferation Treaty (NPT) and several export control agreements show that it is possible to conclude and implement security related agreements when many actors, including industry, are involved. These agreements involve cooperation among governments, industries and national and international agencies. They also require that governments impose regulations on industries as well as national implementation measures. The success of the CWC was partly due to the support of the chemical industry, which resulted in some measure from the fact that they were valued participants in the formulation of the CWC. Some attribute the reasons for failure of the BWC verification protocol in part to the lack of consultation process with the industry during the negotiations. Similarly, in a multilateral agreement on container security there should be incentives to make different stakeholders cooperate. It could also contain provisions similar to other agreements that allow states to assist each other in developing their knowledge base and technical abilities regarding container security.

#### The Code should seek to achieve private sector involvement and universal adoption

Dahlman et al, OD Science Applications, Sweden, 5

(Ola, Jenifer Mackby, Bernard Sitt, Andre Poucet, Arend Meerburg,

Bernard Massinon, Edward Ifft, Masahiko Asada, Ralph Alewine

“Container Security: Proposal for a Comprehensive Code of Conduct,”

Defense & Technology Papers are published by the National Defense University Center for Technology, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434718)

The Code as outlined in the Annex is proposed to be an agreement among States. An agreement should be open for adoption by all States and the EU, with the aim of achieving universality. Relevant international organizations such as the World Customs Organization (WCO) and the International Maritime Organization (IMO) should also be closely associated with the Code. States should provide strong incentives for industry to comply with the Code. For example, shipping companies that strictly adhere to a safe container code could pass through an “express lane” that would process their containers more rapidly than those that don’t.

### Plan Popular

#### Plan popular – its perceived as a security issue

Kasperowicz 12 (Pete Kasperowicz is the chief staff writer for The Hill, “House to push port-security measures this week”, <http://thehill.com/blogs/floor-action/house/234511-house-to-push-port-security-measures-this-week>)

The House this week plans to pass a handful of bills aimed at requiring improved coordination between the federal and state governments on port security, and an assessment of remaining security gaps at ports. The Securing Maritime Activities Through Risk-based Targeting for Port Security Act, from Rep. Candice Miller (R-Mich.), would require the Department of Homeland Security (DHS) and the U.S. Coast Guard to cooperate more in their efforts to ensure port security. It would also boost measures overseas to ensure safer cargo, and encourage more cooperation between the federal and local levels. "In an era of tight budgetary times, we must ensure that we are making the best use of limited taxpayer dollars," Miller said earlier this year when she introduced her bill. "My legislation seeks to guard against these threats in a risk-based, coordinated way that enhances the programs in place to protect our maritime borders." Her bill, H.R. 4251, would require DHS to submit a plan for improved coordination to Congress by July 1, 2014. Another bill, from Rep. Janice Hahn (D-Calif.), would require DHS to submit another report that assesses gaps in port security, as well as a plan for addressing those gaps. Her bill, H.R. 4005, is the Gauging American Port Security (GAPS) Act. Also up this week is H.R. 5889, the Nuclear Terrorism Conventions Implementation and Safety of Maritime Navigation Act. This bill from House Judiciary Committee Chairman Lamar Smith (R-Texas) would make it easier to capture suspected terrorists at sea, and increases penalties against anyone trying to use weapons of mass destruction from or against maritime vessels, or against fixed maritime platforms. The House is also expected to pass a bill that would make it easier for workers in marine facilities or at sea to renew their Transportation Worker Identification Credentials (TWICs). Currently, these workers have to appear twice at an enrollment center to get this credential. The bill — HR. 3173, from Rep. Steve Scalise (R-La.) — would reduce that to one visit. While not related to maritime security, the House will also approve H.R. 1447, which would require DHS to establish an Aviation Security Advisory Committee to advise on security matters. That bill is from Rep. Bennie Thompson (D-Miss.). These and other bills will be brought up under a suspension of House rules, usually reserved for non-controversial bills. Voting on them will start Tuesday night, but some might be considered later in the week.

Plan popular – fear of port attacks empirically proves

Weisman 06 (Jonathan Weisman, Washington Post Staff Writer, “House Passes $7.4 Billion Port Security Bill, The Washington Post, <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/04/AR2006050401672.html>)

The House overwhelmingly approved legislation yesterday to provide $7.4 billion in spending on new port security inspectors, nuclear weapons screening and the development of an automated system to pinpoint high-risk cargo. The 421 to 2 vote came just hours after the White House expressed strong misgivings over the cost and feasibility of the bill. But the lopsided vote underscored how politically sensitive the issue of port security has become since the state-owned Dubai Ports World moved to purchase terminal operations at six major U.S. seaports in February.Republicans had voted several times in the past two years against Democratic proposals to increase funding for port security, saying that enough was already being spent. Indeed, White House officials repeated that assertion yesterday in a policy statement that depicted the House bill as overly generous and technologically unrealistic.But the furor over the Dubai deal brought the two parties together on bipartisan port security legislation. Only two House members opposed the measure yesterday, Rep. Jeff Flake (R-Ariz.), who said the price tag is too high, and Rep. Edward J. Markey (D-Mass.), who contended that the bill does not go far enough to ensure the safety of vulnerable seaports."House Republicans will continue to do what is right to protect American families and prevent a tragedy like September 11th from occurring ever again," said House Speaker J. Dennis Hastert (R-Ill.). "We understand that we must secure our ports in order to protect our citizens."But House Republicans blocked consideration of a Democratic amendment that would have required that all cargo be screened before it leaves foreign ports for the United States. The Senate Homeland Security Committee, in drafting its companion bill earlier this week, added a pilot program at three foreign ports to test the feasibility of 100 percent screening.House GOP leaders called Democratic push unreasonable."One hundred percent screening of every container will shut down worldwide shipping overnight," said House Majority Leader [John A. Boehner](http://projects.washingtonpost.com/congress/members/b000589/) (R-Ohio). He added that a House-passed feasibility study is a "practical, common-sense approach to the issue."Democrats countered that they will continue to push more robust legislation.

"All it takes is one atomic or radiological bomb to make 9/11 look like a firecracker," said [Rep. Jerrold Nadler](http://projects.washingtonpost.com/congress/members/n000002/) (D-N.Y.). "If we really want to make this country safer, we must demand that before any container is put on a ship bound for the United States, it must be scanned electronically in the foreign port. It's too late if we find a nuclear bomb in Los Angeles or New York." Providing an additional $7.4 billion over the next five years, the House bill would bolster the Department of Homeland Security's Domestic Nuclear Detection Office, requiring the deployment of nuclear and radiological detection systems in all domestic seaports. It would set up new tracking systems for discovering and monitoring high-risk cargo and would accelerate the creation of a transportation-worker identification card. New port-security training and exercises would also be required. The White House's Office of Management and Budget expressed concern over what it called the measure's "serious resource implications," charging in a statement of policy that it would tie the hands of the Department of Homeland Security in bureaucratic red tape.The required deployment of advanced radiation detectors by September 2007 "might not be feasible given the current state of detector acquisition, installation, and development," the White House said in a statement. It added that $400 million a year in dedicated port security grants would be unnecessary and wasteful.

Nonetheless, White House officials stopped short of issuing a veto threat on legislation that appears destined for speedy enactment. Four and a half years after the Sept. 11, 2001, attacks, port security has become an unlikely political issue. The same coalition of liberal interest groups and labor unions that helped kill President Bush's Social Security proposals has launched a national campaign to portray Republicans as opposing port security, through home-district appearances and radio advertisements. The Department of Homeland Security currently opens for inspection 6 percent of the 11 million cargo containers that enter U.S. seaports annually. But all cargo manifests are examined, as is "high-risk cargo," which is identified through an automated targeting system. Republican leaders said going much further than the House bill would slow the flow of international trade and would cost U.S. jobs. The issue came to the fore with the Dubai port deal. Bowing to intense pressure, Dubai Ports World announced in March that it would sell to an American firm its U.S. operations at ports in Baltimore, New York, Newark, Philadelphia, Miami and New Orleans. But two months later, no deal has been struck.

### Plan Unpopular – DHS

#### Container security is unpopular with the DHS

Nadler 12 (Jerrold Nadler is the [U.S. Representative](http://en.wikipedia.org/wiki/United_States_House_of_Representatives) for [New York's 8th congressional district](http://en.wikipedia.org/wiki/New_York%27s_8th_congressional_district), serving since 1992, “Cargo, the Terrorists’ Trojan Horse”, http://www.nytimes.com/2012/06/27/opinion/the-dangerous-delay-on-port-security.html?\_r=1)

Over the years, terrorists have shown themselves to be frighteningly inventive. They have hidden explosives in printer cartridges transported by air and embedded explosives in the shoes and underwear of airline passengers. The cargo containers arriving on ships from foreign ports offer terrorists a Trojan horse for a devastating attack on the United States. As the Harvard political scientist Graham T. Allison has put it, a nuclear attack is “far more likely to arrive in a cargo container than on the tip of a missile.” But for the past five years, the Department of Homeland Security has done little to counter this threat and instead has wasted precious time arguing that it would be too expensive and too difficult, logistically and diplomatically, to comply with the law. This is unacceptable.

### Privatization CP – Solvency

#### The Private Sector can do the plan

Isenberg**,** May 26,2012**,** David Isenberg- is an independent, Washington-D.C. based analyst and writer on military, foreign policy, national and international security issue, “The Rise of Private Maritime Security Companies”, http://www.cato.org/publications/commentary/rise-private-maritime-security-companies

**The number of companies who have jumped into the deep blue sea to offer armed guards and other private security services for commercial shippers who fear pirate attacks has risen sharply the past few years. Many new companies have been formed in this area since 2008** and many existing PSCs have refocused on maritime security. Land based private security has vacillated between being called private military companies (PMC's) or private security companies (PSC's). All have been faced with media scrutiny, controversy and varying degrees of helpful and unhelpful legislation. Although the provision of lethal force by private services rather than government services is neither new or even unexpected on land it seems to be more complicated on the ocean and in international waters. Maritime security has existed to protect slow moving oil drilling equipment, private luxury yachts and even undersea cable laying projects. The industry was word of mouth, providers were known by their past clients and there was little demand by traditional shipping companies. The spike in attacks in 2008 forced ship owners and charterers to find ways to reduce risk and rapidly increasing "exception" insurance premiums for routes like the Gulf of Aden and a rapidly expanding piracy zone in the Indian Ocean

#### Private maritime security companies increasing now

Isenberg 5-26-12 David Isenberg, independent, Washington-D.C. based analyst and writer on military, foreign policy, national and international security issues and the author of Shadow Force: Private Security Contractors in Iraq. He is an expert in U.S. defense policy , WMD proliferation, terrorism, homeland security, peace operations, the intelligence community, international arms trade, small arms proliferation, private military companies, biological weapons, and general arms control issues. Isenberg's blog, The PMSC Observer, focuses on private military and security contracting. “The rise of private maritime security companies” Somalia Report, Cato Institute, <http://www.cato.org/publications/commentary/rise-private-maritime-security-companies>

The number of companies who have jumped into the deep blue sea to offer armed guards and other private security services for commercial shippers who fear pirate attacks has risen sharply the past few years. Many new companies have been formed in this area since 2008 and many existing PSCs have refocused on maritime security. Land based private security has vacillated between being called private military companies (PMC's) or private security companies (PSC's). All have been faced with media scrutiny, controversy and varying degrees of helpful and unhelpful legislation. Although the provision of lethal force by private services rather than government services neither new nor even unexpected on land it seems to be more complicated on the ocean and in international waters.

#### Public-Private partnerships are key to solve port security

Weinberg Et al., Partner, 2003(Jim, Mark Gerencser, and Don Vincent “Port Security War Game Implications for U.S. Supply Chains” Report by Booz Allen Hamilton http://www.booz.com/media/uploads/Port\_Security\_War\_Game.pdf)

Public-Private partnerships are essential Global trade resiliency in the face of an ambiguous, unceasing terrorist threat requires new solutions and partnerships that only a fully engaged public and private sector can address. Specifically, business and government need to work together in new and perhaps unfamiliar ways to prevent tampering with cargo. Participants concluded, for example, that international standards are required for preloading container inspections; government must take the lead on this initiative. Industry leadership, on the other hand, is essential to leverage technology such as GPS tracking devices, e-seals, smart containers, and in-transit radiation detection systems that can enhance the ability to track and monitor the integrity of cargo in transit. At discharge points, national security standards for perimeter control and employee credentialing are shared public/private sector responsibilities.

#### Increasing Liability is key – voluntary measures are key

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

In the area of security, there are many reasons to prefer liability to regulation or direct government provision. Flexibility is one advantage. Companies face varying degrees of threats, and individual businesses are often in the best position to know where their weaknesses lie. Uniform regulation may lead to too much security in some sectors and not enough in others. Relying on incentives rather than regulation also guards against the real possibility that regulators will be “captured” by those they supervise. The history of regulation is littered with rules designed to stifle competitors instead of enhance public welfare. Finally, regulation can lead to an unjust distribution of costs, with taxpayers or companies that face few threats subsidizing the security of firms that engage in riskier behavior.

#### Voluntary incentives are key to improving security while maintaining economic efficiency.

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

Second, where rules and regulations are necessary, they should be as open-ended as possible. In such cases, policymakers should set security goals and verify how well companies meet them, not mandate specific technologies or processes. Positive incentives should be considered to encourage companies to be vigilant and to guard against regulations becoming a best practices ceiling, rather than a floor. For example, instead of merely mandating specific intrusion-detection technology for cargo containers, DHS could offer bounties to companies that uncover terrorists or weapons. When the government is seeking to develop new security technologies, it should consider offering bonuses and contracts to the first company that can develop the desired product or meet the specified goal—avoiding “seed money” research grants that are too often awarded on the basis of political criteria.16 Third, policymakers should be aware that securing the trading system against terrorism is a regrettable but real cost of doing business internationally. The prices of imported goods should reflect those costs. The United States benefits from imports when their price and/or quality advantage outweighs their total cost, including the cost of transportation and security. Expansive taxpayer subsidies for commercial security may distort economic decisions and prompt companies to make unwise investments. At the same time, however, it is important that the cost of new security measures be justified by their safety benefits. “Security” should never become an excuse for protectionism.

#### Privatized ports are key to streamlined operations and reduce coercion.

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

America’s ports also deserve scrutiny in terms of subsidies and ownership. Public port authorities own all major U.S. seaports and operate many of them. (A 1990 report by the American Association of Port Authorities showed that 30 percent of the 66 port authorities surveyed were operating at a loss.) As a study by the Reason Foundation reported, government-owned and -operated ports face many problems. In the post-9/11 environment, streamlined port operations will be critical to offset security-driven efficiency losses. Yet publicly owned and operated ports are regularly subjected to political interference and have weakened incentives to operate efficiently because they are insulated from commercial competitive pressures. Public ports have also been known to soak up funds from local governments and drag down local economies. Conversely, relatively efficient public ports are often targeted by local governments that want to siphon off “surplus” funds.17 Finally, security policy should always be developed with an eye toward the U.S. Constitution. Reducing the risk of terrorist attack on or through the trading system is an important objective, but it must be achieved within a framework of law that protects the civil liberties and privacy of U.S. citizens.

#### The Military Proves that TAV is feasible

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

The ideal security system would offer what experts call “Total Asset Visibility and Authentication”— integrated procedures and technologies that safeguard cargos at all stages of transport. Total Asset Visibility and Authentication would require (1) loading of shipments in a secure facility, by authenticated personnel; (2) verification of the contents of a shipment; (3) security in transit; (4) transmitting the content and manifest information to Customs and stakeholders upon loading; (5) the ability to identify container tampering; and (6) a way for Customs to provide verification of a container’s contents and integrity in a nonintrusive manner at the point of entry. 20 Such a system is not without precedent. The Department of Defense’s Total Asset Visibility Network (TAV) uses radio frequency tags with full electronic container manifests attached to containers, wireless tag readers located at checkpoints around the world, and a computerized system to track and monitor the status of the containers. The TAV system uses checkpoints at more than 400 locations in 36 countries—military and commercial seaports, airports, rail terminals, and military bases—to track the movement of some 250,000 conveyances.21

#### No Total Asset Visibility Now

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

Although the U.S. government is exploring the move toward a TAV system for private commerce, the current programs have not moved much beyond demonstration and testing. This does not mean that security officials have been derelict. Securing the trading system is an enormously complex and expensive task—one that could not have been reasonably completed in the two years since the attacks on New York and Washington. The approach has been to create multiple programs that focus on different components of the trading system, from loading to delivery, for several modes of transport. Those programs will naturally take time to implement.

#### Federal Involvement in directives is key

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

The security of global trade is a never-ending project, one in which the government has a legitimate and leading role to play. The country must continue to be alert for ways to enhance security without closing borders. This will require an ongoing assessment of the costs and benefits of current and future trade-security initiatives. It will mean maintaining an openness to new technologies and the right incentives to develop them. It will rely on open lines of communication between intelligence agencies, homeland security agencies, ports, businesses, and state, local, and foreign governments. Above all, an effective risk-reduction strategy will require a recognition that although the federal government can coordinate America’s efforts, it cannot and should not be the sole provider of security. Private companies will, of necessity, be on the front lines of this conflict. Where regulations are necessary, companies should specify goals, set standards, and gauge progress rather than micromanage behavior. Companies should be encouraged not only to follow the letter of government directives, but to become responsible stakeholders in the terrorism prevention business. Vigilance must become a mindset, not just a checkbox on a list of rules. In this endeavor, stasis will be the enemy of safety. Terrorists will study whatever measures are adopted. They will probe for weaknesses and eventually find some. Successful attacks are probably inevitable. Yet a tough and adaptable trade-security system can give policymakers the confidence to keep the engine of trade running when something does go wrong. And with each incident, policymakers, agencies, and companies will have the opportunity to learn from their mistakes and make future attacks less likely.

### Protectionism Link

#### The plan is perceived as protectionism.

Lukas, 4/8/2004 (Aaron, “Protection without Protectionism: Reconciling Trade and Homeland Security” Center for Trade Policy Studies CATO Trade Policy Analysis No 27.)

Finally, although the legislative threat of protectionism masquerading as security lies largely in the future, DHS is already spending scarce resources on projects of little value. In 2003, for example, Customs seized more than $160 million in apparel shipments from China that violated quota restrictions.86 Despite the fact that the United States will be scrapping its quotas in less than a year, Rep. Sue Myrick (RNC) reports working with Customs to fund the development of a “textile tracer” that would determine the origin of U.S. textile imports.87 Customs is struggling to search shipping containers for WMD, yet Myrick boasts that she has “also secured $9.5 million in funding to hire additional custom agents to guard our borders against these illegal textile goods coming in from other countries.”88 Considering what is at stake, there are better ways that those millions could be spent than “protecting” Americans from low-cost clothing.

### Spending Link

#### Current tech incredibly expensive and ineffective

Carafano and Zuckerman, 12 (James Jay Carafano and Jessica Zuckerman, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies and Director, Douglas and Sarah Allison Center for Foreign Policy Studies and Research Associate, Douglas and Sarah Allison Center for Foreign Policy Studies, “Maritime Cargo Scanning Folly: Bad for the Economy, Wrong for Security”, Heritage foundation, <http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate>)

Cost and infrastructure are also important factors. A single x-ray scanner, the most common technology used for cargo screening, can have a price tag of $4.5 million, plus an estimated annual operating cost of $200,000, not to mention the roughly $600,000 per year for the personnel required to run the equipment and examine the results.[3]

Likewise, the mere placement of scanners can also prove to cause logistical problems, as many ports were not built with natural bottlenecks through which all cargo passes. With today’s economy relying heavily on the timely and efficient

movement of goods, and such logistical delays could amount to around $500 billion in total profit loss. And once scanning technology is installed, it may encounter multiple problems, such as incompatibility with previous technologies, frequent outages due to weather, and insufficient communication infrastructure to transmit electronic data to the U.S. National Targeting Center-Cargo, where it is assessed.

### States (Local) CP Solvency

#### States solve best – Local knowledge of ports is key.

Keefer, J.D, 2008 (Wendy J. “Container Port Security: A Layered Defense Strategy to Protect The Homeland and The International Supply Chain” Campbell Law Review Vol. 30:139)

To consider competently any proposed method for undertaking to secure container shipments, an understanding must exist about the functioning of the particular port, the most likely risks of criminal activity faced by that port, and the resources available for combating those activities. A port that primarily handles cargo faces different issues than one typically used for passenger travel. Similarly, the volume of cargo or passengers will impact how the port operates, as well as what types of security measures are even feasible. In this regard, the current status of the ports in Charleston, South Carolina and Wilmington, North Carolina is instructive of the need for container security for shipments to these ports.

### Topicality Violation – RFIDs Aren’t Transportation Infrastructure

#### “Transportation infrastructure” is only the underlying delivery structures for goods and services – the plan doesn’t invest in those structures.

Trimbath 9 (Dr. Susanne, Senior Research Economist in Capital Market Studies at Milken Institute, Senior Advisor – United States Chamber of Commerce, and Professor of Economics and Accounting – Bellvue University, “Transportation Infrastructure: Paving the Way”, <http://www.uschamber.com/sites/default/files/issues/infrastructur> e/files/2009TPI\_Update\_Economics\_White\_Paper\_110712.pdf)

V. Paving the Way Forward

The strategy applied by the US Chamber of Commerce for the infrastructure performance index project presents a model for developing the way forward. A stakeholder-centric approach allows you to measure the right things, communicate to the people in a language they understand and get to ACTION faster. The process, detailed in the Technical Report last summer (US Chamber 2010), is basically this:

1. Clearly define “transportation infrastructure” as the underlying structures that support the delivery of inputs to places of production, goods and services to customers, and customers to marketplaces. The structures are:

- Transit

- Highways

- Airports

- Railways

- Waterways (Ports)

- Intermodal Links

#### Voting issue --- they expand the topic from “increasing” infrastructure to “altering” it through deregaulation, liberalization, or privatization --- makes Neg research impossible, especially because predictable ground assumes current methods

### Trade DA

#### Increased Security Related costs kill the economy

Frittelli, Specialist in Transportation Resources, Science, and Industry Division, 5/27/2005(John F. “Port and Maritime Security: Background and Issues for Congress” CRS Report to Congress http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA453735)

The container shipping system is designed for speed and efficiency. Transportation services are a critical component of the global, low-inventory (i.e., just-in-time) distribution model that many manufacturers have adopted. Most industries in the United States use some imported components from overseas suppliers. By bringing parts to a plant just before they are needed for assembly, manufacturers can save money on warehouse space and inventory carrying costs. Transport efficiencies permit warehouse requirements to be minimized. Lean inventories in turn have contributed to business productivity. From 1980 to 2000, according to one study, business logistics costs dropped from 16.1% of U.S. GDP to 10.1%. 15 Given the dependence of the United States and the global economy on a highly efficient maritime transportation system, many experts acknowledge that slowing the flow of trade to inspect all inbound containers, or at least a statistically significant random selection would be “economically intolerable.” 16 Supply chain analysts are concerned that increased security-related delay at seaports could threaten the efficiency gains achieved in inventory management over the past two decades by forcing companies to hold larger inventories.

#### Economic decline increases the risk of war—strong statistical support.

Royal 10 — Jedidiah Royal, Director of Cooperative Threat Reduction at the U.S. Department of Defense, M.Phil. Candidate at the University of New South Wales, 2010 (“Economic Integration, Economic Signalling and the Problem of Economic Crises,” *Economics of War and Peace: Economic, Legal and Political Perspectives*, Edited by Ben Goldsmith and Jurgen Brauer, Published by Emerald Group Publishing, ISBN 0857240048, p. 213-215)

Less intuitive is how periods of economic decline may increase the likelihood of external conflict. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent states. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow.

First, on the systemic level, Pollins (2008) advances Modelski and Thompson's (1996) work on leadership cycle theory, finding that rhythms in the global economy are associated with the rise and fall of a pre-eminent power and the often bloody transition from one pre-eminent leader to the next. As such, exogenous shocks such as economic crises could usher in a redistribution of relative power (see also Gilpin. 1981) that leads to uncertainty about power balances, increasing the risk of miscalculation (Feaver, 1995). Alternatively, even a relatively certain redistribution of power could lead to a permissive environment for conflict as a rising power may seek to challenge a declining power (Werner. 1999). Separately, Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown.

Second, on a dyadic level, Copeland's (1996, 2000) theory of trade expectations suggests that 'future expectation of trade' is a significant variable in understanding economic conditions and security behaviour of states. He argues that interdependent states are likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However, if the expectations of future trade decline, particularly for difficult [end page 213] to replace items such as energy resources, the likelihood for conflict increases, as states will be inclined to use force to gain access to those resources. Crises could potentially be the trigger for decreased trade expectations either on its own or because it triggers protectionist moves by interdependent states.4

Third, others have considered the link between economic decline and external armed conflict at a national level. Blomberg and Hess (2002) find a strong correlation between internal conflict and external conflict, particularly during periods of economic downturn. They write,

The linkages between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict tends to spawn internal conflict, which in turn returns the favour. Moreover, the presence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other. (Blomberg & Hess, 2002. p. 89)

Economic decline has also been linked with an increase in the likelihood of terrorism (Blomberg, Hess, & Weerapana, 2004), which has the capacity to spill across borders and lead to external tensions.

Furthermore, crises generally reduce the popularity of a sitting government. “Diversionary theory" suggests that, when facing unpopularity arising from economic decline, sitting governments have increased incentives to fabricate external military conflicts to create a 'rally around the flag' effect. Wang (1996), DeRouen (1995). and Blomberg, Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force are at least indirectly correlated. Gelpi (1997), Miller (1999), and Kisangani and Pickering (2009) suggest that the tendency towards diversionary tactics are greater for democratic states than autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office due to lack of domestic support. DeRouen (2000) has provided evidence showing that periods of weak economic performance in the United States, and thus weak Presidential popularity, are statistically linked to an increase in the use of force.

In summary, recent economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science scholarship links economic decline with external conflict at systemic, dyadic and national levels.5 This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention.

This observation is not contradictory to other perspectives that link economic interdependence with a decrease in the likelihood of external conflict, such as those mentioned in the first paragraph of this chapter. [end page 214] Those studies tend to focus on dyadic interdependence instead of global interdependence and do not specifically consider the occurrence of and conditions created by economic crises. As such, the view presented here should be considered ancillary to those views.

### EXT – Trade DA Links

#### Expanding port security undermines global trade

Keefer, J.D, 2008 (Wendy J. “Container Port Security: A Layered Defense Strategy to Protect The Homeland and The International Supply Chain” Campbell Law Review Vol. 30:139)

The only way wholly to ensure terrorists are unable to use containers to import weapons, other supplies or even would-be terrorists themselves is greater, indeed complete, physical inspection of incoming containers. Such inspections would need to be conducted prior to the carrying vessel’s entry into U.S. waters. Searches of all entering containers — or even inspection of any statistically significant number of containers — is extremely impractical. The impracticality of large scale inspections is clear when one considers that even now only about 5% 63 of containers entering United States ports are examined to identify their contents. Any large scale expansion of the number of containers examined — whether using non-intrusive imaging technology or involving an actual physical search — would be overly burdensome on global trade. Indeed, such security measures may themselves serve one of the potential terrorist goals by slowing maritime trade to an economically unacceptable level. 64

#### Link - Increasing port security is an economic burden.

Beltzer, 11. (Michael H. Beltzer, Associate Professor of Industrial Relations in the Department of Interdisciplinary Studies of the College of Liberal Arts and Sciences at Wayne State University. He also is a Research Scientist at the University of Michigan's Institute of Labor and Industrial Relations, and is Associate Director of the Alfred P. Sloan Foundation's Trucking Industry ProgramSupply Chain Security: Agency Theory and Port Drayage Drivers,

Economic Labor Relations Review, <http://search.proquest.com/docview/870060083/fulltext>)

Most solutions to date have been to increase surveillance and enforcement and to increase use of technology in this effort, and the economic burden is substantial. In addition, while the economic benefits flow to a narrow sector of the economy (the security and information technology sectors), the costs are borne by the public in the form of higher prices and distortions in allocative efficiency. Further, according the Secretary of DHS, 'guarding against every terror risk would bankrupt the US' (Lipton 2006). Martonosi, Ortiz, and Willis imply that the cost of 100 per cent inspection of inbound containers would be approximately $900 million annually (Martonosi et al. 2006). The cost of compliance with extremely high security standards would result in both increased cost to consumers and reduced economic activity (deadweight loss) and thus produce serious negative macroeconomic effects - all of which have much greater consequences since the global financial meltdown occurred in 2007-2010.

#### Link: Maritime crime is inevitable and attempting to stop it will only hurt the US economy

Lukas, April 8, 2004, Aaron Lukas- a former policy analyst with Cato's Center for Trade Policy Studies. He conducts research in areas such as the intersection between trade and security, the taxation of electronic commerce, and the cost of economic sanctions. Lukas first joined the Trade Center in 1998. In 2002-2003, he served as chief speechwriter and strategic adviser for U.S. Trade Representative Robert B. Zoellick, “Protection without Protectionism”, The Cato Institute, <http://www.cato.org/pubs/tpa/tpa-027.pdf>

Protecting America’s economy and people from assaults on trade is a necessary venture. Yet there are limits to what can be done. Security, like other goods, is subject to the law of diminishing returns. The United States could conceivably seal its borders and cease trading with other nations. Halting all trade, now and forever, would eliminate the threat of a bomb in a cargo container. But exchanging the possibility of a terror attack for the certainty of a poorer nation—and thereby advancing an end that America’s enemies seek—would not be a wise course of action. We must instead recognize the inevitable tradeoffs between security and efficiency and seek to balance costs with benefits. Americans have the right to do business with anyone they choose—and that right should only be restricted in extraordinary circumstances. In brief, the challenge for U.S. policymakers is to improve security while minimizing the loss of liberty and the benefits of economic openness. The truth is that the United States will never be completely secure. Opportunities to exploit the trading system for nefarious ends will always exist. Although risk cannot be eliminated, it can be managed. A layered system can have safeguards that build upon one another at all stages of trade—from packing, to ports, to shipping, to border controls, to personnel checks. No single component of the system will be infallible, but taken together, overlapping precautions make a major tragedy unlikely. In the event that defenses fail and a terror attack on (or delivered via) the institutions of global trade occurs, robust layered security can minimize disruption by giving officials the confidence to respond without shutting down commerce altogether. The optimal balance between security and openness is difficult to determine even in the best of times. Achieving that balance is even more difficult because of the temptation for domestic interests to press for measures that unfairly hinder their foreign competitors without appreciably improving U.S. security. Such protectionism masquerading as homeland defense is more than a theoretical possibility. Legislation has been introduced in Congress, for example, that would require all inbound ships to have their cargos screened at an offshore location before landing in the United States. Such draconian approaches would hobble the U.S. economy while providing little additional security.

#### Physically inspecting containers would hurt US trade

Knight ’03 (Sam Knight. Sam Knight has been working with the New Security Issues Programme at Chatham House.

“The Bomb in the Box.” Chatham House: the World Today. http://search.proquest.com/education/docview/234225047/1376FF0AD42784B0113/10?accountid=11091)

The first challenge is that of scale. Container shipping is big. Seven million TEU - twenty-foot equivalent units, the standard measurement for the container trade - pass through Britain's ports each year. Given that containers are increasingly forty feet long, that means four and a half million boxes. One every seven seconds. Every year, forty eight million full containers pass between the world's seaports, carrying around ninety percent of the planet's general cargo. The latest container ships move up to 6,800 TEU, stacked several stories high. Estimates of the total annual worldwide movement of containers, empty and full, vary between seventy and two hundred million TEU. You could fit the population of Britain into just three and a half million. These numbers indicate the size of the task facing the world's customs and the need to limit the more hysterical security proposals to allow trade to flow. In America, just two percent of containers are physically inspected at present. Any attempt to raise that quota would pose serious obstacles to the $2 billion worth of trade that passes through US ports daily.

#### Increase in Port Security could greatly affect economy

McClure, 2007, [George F. McClure, Technology Policy editor for IEEE-USA TodayÔøΩs Engineer and a member of IEEE-USA's Committee on Transportation and Aerospace policy, ÔøΩHow Safe are our Ports?ÔøΩ, TodayÔøΩs Engineer, <http://www.todaysengineer.org/2007/Sep/port-security.asp>]

**U.S. ports handle more than 2 billion tons of domestic and import/export cargo per year, $1.3 billion worth of goods move in and out of U.S. ports every day. Interference with their function would be disruptive to the U.S. economy**. However, terrorist activity could destroy port facilities or use them as a channel to move materials into the United States for other destinations.

#### 100% screening link- Ports still insecure because no 100% inspection

McClure, 2007 [George F. McClure, Technology Policy editor for IEEE-USA TodayÔøΩs Engineer and a member of IEEE-USA's Committee on Transportation and Aerospace policy, ÔøΩHow Safe are our Ports?ÔøΩ, TodayÔøΩs Engineer, <http://www.todaysengineer.org/2007/Sep/port-security.asp>]

Manifest reviews are completed for all shipments at least 24 hours before containers bound for the U.S. are loaded on ships at foreign ports. **About 5 percent of containers are actually inspected, based on risk profiles**. Legislators have proposed 100 percent scanning of containers, either overseas or at U.S. ports and A RAND study concludes that **100 percent inspection would be warranted only if the threat of damage from potential terrorism was quite high** [Another view is **that 100 percent screening would be expensive and impractica**l ‚Äî not in keeping with the threat [‚Äî and seen as more costly than the potential risk, one must conclude.

#### Technology vital scanning packages nonexistent- cause billions in economic loss

Carafano and Zuckerman, 12 (James Jay Carafano and Jessica Zuckerman, Deputy Director, The Kathryn and Shelby Cullom Davis Institute for International Studies and Director, Douglas and Sarah Allison Center for Foreign Policy Studies and Research Associate, Douglas and Sarah Allison Center for Foreign Policy Studies, “Maritime Cargo Scanning Folly: Bad for the Economy, Wrong for Security”, Heritage foundation, <http://www.heritage.org/research/reports/2012/02/maritime-cargo-port-security-and-the-100-percent-screening-mandate>)

Last week, the Obama Administration released its first ever National Strategy for Global Supply Chain Security. As stated, the main goals of the strategy are to promote the efficient and secure movement of goods and foster a resilient supply chain. Maintaining a secure and resilient supply chain is certainly critical to ensuring the prosperity of the United States’ $14.6 trillion economy. However, existing legislation governing maritime cargo transit and port security directly contradicts the goals of this strategy. Given the extensive economic importance of the maritime supply chain, the vulnerability of maritime cargo to terrorist and other malicious attacks has long been a concern. With this concern heightened after 9/11, Congress and the Administration moved to create a risk-based approach to strengthen maritime security centered on analyzing cargo attributes, such as contents and origin of the cargo container, to single out high-risk cargo for further inspection. While screening calls for cargo to be assessed for risk on the basis of contents, origin, and other attributes, scanning means that each of the approximately 11.6 million maritime cargo security containers entering U.S. ports each year must be physically scanned. With many maritime cargo increasingly containerized in recent decades, typical maritime cargo containers often measure some 40 feet in length. One key issue regarding maritime cargo screening is, therefore, one of scale. While the basic technology exists to effectively screen cargo containers, the expanded technology necessary to perform this function on large containerized cargo largely does not. Cost and infrastructure are also important factors. A single x-ray scanner, the most common technology used for cargo screening, can have a price tag of $4.5 million, plus an estimated annual operating cost of $200,000, not to mention the roughly $600,000 per year for the personnel required to run the equipment and examine the results.[3] Likewise, the mere placement of scanners can also prove to cause logistical problems, as many ports were not built with natural bottlenecks through which all cargo passes. With today’s economy relying heavily on the timely and efficient movement of goods, and such logistical delays could amount to around $500 billion in total profit loss. And once scanning technology is installed, it may encounter multiple problems, such as incompatibility with previous technologies, frequent outages due to weather, and insufficient communication infrastructure to transmit electronic

### EXT – Trade DA – Ports Key to Trade

#### 90% of world trade done through the maritime sector

Samsa 6-27-12 (South African Maritime Safety Authority, Seafarers crucial as 90% of world trade done through shipping, <http://www.bizcommunity.com/Article/196/593/77569.html>

According to *The New Age*, the South African Maritime Safety Authority (Samsa) celebrated June 25 - the International Day for Seafarers - paying tribute to the men and women who spend their lives at sea. It is estimated that 90% of world trade goes through the sea and is facilitated by 1.5 million seafarers.

"As shipping is responsible for the carriage of more than 90% of the world trade, it is the seafarers who ensure the smooth running of the shipping engines and the safe delivery of essential items and commodities that enhance our lives on a daily basis," Samsa spokesperson Tsietsi Mokhele said, adding that he hopes that resolutions taken at the conference will help fast track initiatives undertaken to address challenges facing the sector, including increasing the number of local seafarers, reports *The New Age*. South Africa prepares to host the country's first maritime industry conference, to be held at the International Convention Centre in Cape Town from July 4, enabling role players and participants to discuss the plight of seafarers and the challenges they face daily in their jobs.   
More than 700 delegates from South Africa and the African continent are expected to attend the conference, *The New Age* says.