### 1ac

#### Contention 1: Inherency

#### Current measures to protect our ports fail

Vesky, 2008 (Jonathan, Port and Maritime Security Pg 27-28)

 A major concern for Congress is assessing whether the nation is doing enough and fast enough to deter a terrorist attack in the maritime domain. Despite the progress that has been made in strengthening port security thus far, many security officials still describe seaports as "wide open" and "very vulnerable" to terrorist attack.12 Seaports, along with air cargo, general aviation, and mass transit, were identified in a April 2003 GAO report as the "major vulnerabilities" remaining in the nation's transportation system. The GAO found that "an effective port security environment may be many years away." While many agree that CSI, C-TPAT, OSC, and MDA, are sound strategies for addressing the threat, they contend that these programs represent only a framework for building a maritime security regime, and that significant gaps in security still remain. In the words of one security expert,14

overseas point of origin.17 Finding the right balance between improving cargo security to desired levels without unduly impeding the legitimate flow of commerce is a difficult issue.

**Current risk model for Port Security Grants needs to be reformed to more adequately reflect infrastructure**

GAO, 11/11/2011 (“PORT SECURITY GRANT PROGRAM: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened” United States Government Accountability Office http://www.gao.gov/products/GAO-12-47)

Although FEMA has taken the first step towards improving how port vulnerability is measured in the PSGP risk model, further improvements are needed to ensure that the vulnerability score for a specific port is responsive to changes in security that may occur in that port—such as the implementation of new security measures. The fiscal year 2011 vulnerability index does not provide a mechanism to account for how new security measures—such as the installation of cameras or the provision of additional training to security officials —affect a port’s vulnerability, even if those security measures were funded using PSGP grant dollars. This limitation is due to the fact that the data elements within the vulnerability index are counts of activities, which recognize the number of activities that may occur—such as how many ferry passengers board a ferry—but do not account for the protective actions taken to secure them. For example, if a port installed security cameras throughout a ferry system to monitor vessel or ferry passenger activity, one would expect to reduce the ferry system’s vulnerability to attack. However, because the “ferry passenger” data element within the model’s vulnerability index is simply a count of passengers utilizing the ferry system and is not a reflection of the security measures in place to protect the ferry system, the new camera system would not reduce the port’s vulnerability score as calculated by the risk model. Thus, with this type of measure, in this example, a port could only reduce its vulnerability score by reducing the number of passengers utilizing the ferry system. The model’s robustness is thereby limited because activity counts do not reflect improvements made to port security. It is important to note that some security improvements may be captured by the inclusion of the Coast Guard’s Maritime Security Risk Analysis Model (MSRAM) results in the PSGP risk model.27 The MSRAM data— which are updated annually—provide information to the model on the percentage of national high-risk assets that reside within each port. However, MSRAM does not account for all types of security improvements because it is an asset-based model that assesses improvements to individual port assets such as a ferry terminal or a chemical plant. As such, MSRAM is not designed, for example, to evaluate security projects that may affect multiple assets in a port. The National Infrastructure Protection Plan states that when measuring vulnerability, one should describe all protective measures in place and how they reduce vulnerability. FEMA officials reported that capturing data on all security improvements would be challenging due to the need to collect and validate data for all ports included in the PSGP risk model. However, FEMA officials acknowledged the importance of incorporating completed security projects as part of the vulnerability component of the risk model and stated that FEMA will continue to refine its vulnerability assessments. Without accounting for the reductions in vulnerability achieved through new security measures implemented in a port, including those funded through the PSGP, the robustness of the risk model may be limited and not accurately reflect the relative risk of port areas throughout the nation. Instead, the risk model would likely continue to recognize the same ports as the highest risk, regardless of the security improvements made in those ports. In addition, by not accounting for security improvements resulting from PSGP grants, the security benefits of the PSGP are also not recognized. Incorporating completed security projects into the vulnerability component of the risk model could help increase its robustness and more accurately direct allocations to the highest risk port areas.

#### Advantage 1 is the Economy:

#### Security checks will increase in the status quo even absent the plan

Tsilingiris et al, 2007 (P.S., Laboratory for Maritime Transport – National Technical University of Athens, Greece, H. N. Psaraftis Laboratory for Maritime Transport – National Technical University of Athens, Greece, D. V. Lyridis Laboratory for Maritime Transport – National Technical University of Athens, Greece “RFID-enabled Innovative Solutions Promote Container Security” www.­martrans.­org:­8093/­docs/­publ/­REFEREED CONFERE­NCES/­SSE07 tsilingiri­s et al 2007.­pdf)

Contrary to the container ID, seal, and damage check, inspection does not take place in all containers. In the example of a certain EU port we investigated, ca. 2% of all the ocean incoming containers are checked for secu-rity purposes. Truck incoming containers are usually not checked. This check is not homogeneous in the sense that the majority of certain sets of “suspect” containers may be inspected while other non-suspect sets may not be opened at all. This is performed via a decision-support inspection system, which produces a probability inspection function. Variables of the function are cargo data like origin, destination, etc. In essence, this pro-gram resolves the containers that will be checked. The inspection takes place only after the container has been stacked, the operator has adduced declarative docu-ments to the customs, and the container has been stored in the port information system as a stored container. If the decision support system suggests the inspection of the container, the customs broker/clearer communicates with the customs the inspection command. Promptly, the container is “blocked” and the container operator is informed via an XML message. Then, the container is moved to the area where the inspection takes place. When the inspection finishes, a new seal is put to the cleared container, the customs “unblock” the container, and the container is again stacked. Thus, the unblocked container can be retrieved by a trucker. US and EU port operators currently inspect 2-5% of the more than 6 million containers that enter the US per annum. However, since the US fears that containers will be a modus for terrorist attacks, they want to increase the number of inspected containers. This could create chaotic delays as the infrastructure is certainly not ready to handle this.

#### Redundancy in container IDs now – reduces economic efficiency

Tsilingiris et al, 2007 (P.S., Laboratory for Maritime Transport – National Technical University of Athens, Greece, H. N. Psaraftis Laboratory for Maritime Transport – National Technical University of Athens, Greece, D. V. Lyridis Laboratory for Maritime Transport – National Technical University of Athens, Greece “RFID-enabled Innovative Solutions Promote Container Security” www.­martrans.­org:­8093/­docs/­publ/­REFEREED CONFERE­NCES/­SSE07 tsilingiri­s et al 2007.­pdf)

The major objectives of container ID tracking are to perform quickly and with accuracy: (a) container identification; (b) seal check; (c) damage check. With current practices, these tasks are done by multiple players (shippers, forwarders, consignees, etc). Indeed, one stakeholder may perform each task many times (e.g., as we know at a container terminal all (a), (b), and (c) are done at the gate, at the quay, etc.). To make matters worse, the different players do not share the information of the checks and these checks are inevitably repeated. Container identification regards the correct reading (and correct storage of this information) of the markings that associate with the container ID. The principal ID mark-ing of the container and its explanation are depicted in Fig. 3. The container identification system specified in DIN EN ISO 6346 consists solely of the elements shown, which can only be used together: owner code, consisting of three capital letters; product group code, consisting of one of the capital letters U, J or Z; a six-digit registration number; and a check digit. Typically, container ID check is done visually by employees and, rarely, via video check done again by an employee. In any case, human intervention takes place.

#### Any disruption in our maritime commerce would severely damage the economy

Bouchard, 2005 (Joseph F., Former Navy Captain and Doctor of Philosophy in Political Science from Stanford University, 6/15/05, Center for American Progress, http://www.americanprogress.org/issues/2005/06/b815195.html, “New Strategies to Protect America: Safer Ports for a More Secure Economy,”)

The United States is a maritime nation. We rely upon and profit from global commerce worth trillions of dollars. Any major disruption of these worldwide supply chains will instantly create billions of dollars in economic loss and create cascading effects in every corner of the world. Against this backdrop of risk, the Bush administration and its Department of Homeland Security have failed to dedicate sufficient resources to adequately protect the maritime transportation system that is vital to our society, economy and way of life. Port security is currently an unfunded mandate and that situation will deteriorate because the Bush administration plans to eliminate the specific grant program - poorly funded as it is - that supports municipal, state and private sector owners and operators as they attempt to implement security plans required by the MTSA. The Center for American Progress proposes a four-point strategy that will lead to safer ports and make our people and economy more secure. The optimum strategy for protecting maritime transportation requires a risk-based approach to integrating security, consequence reduction, and emergency preparedness and continuity of business into comprehensive plans and programs for enhancing the resilience of the maritime transportation system. Its major features include: Revising Coast Guard maritime facility security regulations and, if necessary, amending MTSA to emphasize risk assessments focused on the threat and consequences of a terrorist attack rather than vulnerability; Increasing attention to risk mitigation, preparedness and continuity of operations to enable the maritime transportation security system to recover quickly in the event of a terrorist attack, reducing the economic consequences of a severe disruption, thereby denying attackers their central strategic goal; Maintaining the existing Port Security Grant Program, creating greater program flexibility for an improved return on investment and increasing annual funding to a minimum of $500 million per year in order to eliminate the current mismatch between strategy and resources and make port security a funded federal mandate; and Establishing a national port security trust fund by dedicating a specific percentage of customs revenue collected on goods flowing through our nation's ports in order to ensure long-term sustainability of our maritime transportation system security. This report focuses on security measures at or near U.S. shores. It is limited in scope to policies and issues directly related to MTSA implementation and its impact on the 361 commercial ports in the United States; roughly 3,700 maritime facilities, including cargo and passenger terminals, in those ports; and approximately 60,000 ships that arrive in U.S. ports annually, including about 8,100 foreign flag vessels. Although cargo, container and supply chain security are mentioned in MTSA, these very important issues will only be tangentially covered. Port security also encompasses what is termed "maritime domain awareness," which includes security on the high seas and abroad. The emphasis is on the Department of Homeland Security (DHS) and the agencies within it, particularly the U.S. Coast Guard, not other federal departments and agencies that play important but supporting roles.

#### And, 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.

#### Efficient port functioning is key to military readiness

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)

National Security Importance. In addition to its economic significance, the marine transportation system is vital for national security. The Departments of Defense and Transportation have designated 17 U.S. seaports as strategic because they are necessary for use by DOD in the event of a major military deployment. Thirteen of these ports are commercial seaports. During Desert Storm, 90% of all military equipment and supplies were shipped from U.S. strategic ports. The deployment required over 312 vessels from 18 commercial and military ports in the United States. As the GAO has reported, “If the strategic ports (or the ships carrying military supplies) were attacked, not only could massive civilian casualties be sustained, but DOD could also lose precious cargo and time and be forced to rely heavily on its overburdened airlift capabilities.” 18

#### Readiness is critical to prevent rivals from lashing out and prevent war

Spencer, 2000 (Jack, Research Fellow at Thomas A. Roe Institute for Economic Policy Studies, “The Facts About Military Readiness”, Heritage Foundation, September 15th, <http://www.heritage.org/Research/Reports/2000/09/BG1394-The-Facts-About-Military-Readiness>)

America's national security requirements dictate that the armed forces must be prepared to defeat groups of adversaries in a given war. America, as the sole remaining superpower, has many enemies. Because attacking America or its interests alone would surely end in defeat for a single nation, these enemies are likely to form alliances. Therefore, basing readiness on American military superiority over any single nation has little saliency. The evidence indicates that the U.S. armed forces are not ready to support America's national security requirements. Moreover, regarding the broader capability to defeat groups of enemies, military readiness has been declining. The National Security Strategy, the U.S. official statement of national security objectives,3 concludes that the United States "must have the capability to deter and, if deterrence fails, defeat large-scale, cross-border aggression in two distant theaters in overlapping time frames."4According to some of the military's highest-ranking officials, however, the United States cannot achieve this goal. Commandant of the Marine Corps General James Jones, former Chief of Naval Operations Admiral Jay Johnson, and Air Force Chief of Staff General Michael Ryan have all expressed serious concerns about their respective services' ability to carry out a two major theater war strategy.5 Recently retired Generals Anthony Zinni of the U.S. Marine Corps and George Joulwan of the U.S. Army have even questioned America's ability to conduct one major theater war the size of the 1991 Gulf War.6 Military readiness is vital because declines in America's military readiness signal to the rest of the world that the United States is not prepared to defend its interests. Therefore, potentially hostile nations will be more likely to lash out against American allies and interests, inevitably leading to U.S. involvement in combat. A high state of military readiness is more likely to deter potentially hostile nations from acting aggressively in regions of vital national interest, thereby preserving peace.

#### Increasing the speed of cargo removal increases economic efficiency

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 issue of port security and how it affects the international supply chain flow is related to manufacturing and logistics operations (Sarathy, 2006). For example, the majority of Aurora Networks products are manufactured and supplied by vendors in the Asia Pacific (APAC) countries. The products are moved in cargo containers (Aurora imports two to three containers a month) and shipped into the port of Oakland, CA. The availability of faster screening technology at the ports mean cargos are cleared faster and delivered to the warehouse (Bottan, 2009). Port screening technology plays an important role in the international supply chain, and adversely affects operations at many U.S. companies (Rice, 2003). Seaports are the backbone of the worldwide commercial traffic (Maritime Security, 2007). The rapid growth of maritime trade creates a continuing need to expand seaports and provide high-quality services (Maritime Security, 2007). At the same time, technological, regulatory, security, and economic trends are placing new demands on seaports and cargo screening technologies.

#### Security Improvements increase the economy by increase speed of current security

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)

Enhanced security has benefits as well as costs. Many experts see economic benefits to tighter control over maritime commerce. Resources put towards seaport security can also reduce cargo theft, narcotic and migrant smuggling, trade law violations, the accidental introduction of invasive species, and the cost of cargo insurance. Improved planning for responding to a terrorist attack at a seaport could also improve responses to other emergencies, such as natural disasters or transportation accidents. New technologies intended to convert the sea container into a “smart box,” such as electronic seals, sensors, or tracking devices, could also improve shipment integrity, help carriers improve their equipment utilization, and help cargo owners track their shipments. In response to the terrorist threat, the CBP has accelerated development of its new information management system, the Automated Commercial Environment (ACE). This system will assist CBP in evaluating cargo manifest information for high risk shipments but will also speed the customs filing process for U.S. importers. 17

#### Advantage Two is Terrorism

#### Al Qaida is targeting maritime transport

Goslin, 2012 (Charles Goslin, Vice President of International Operations for Duos Technologies, Inc. senior advisor to the Regional Joint Terrorism Task Forces (JTTF) in the U.S. Duos Technology Library “Maritime and Port Security White Paper” http://www.duostechnologies.com/DownloadCenter/WP-MaritimeAndPoratSecurity.pdf )

Global trade is dependent mainly on maritime transport. It is estimated that more than 46,000 vessels and 4,000 ports make up the world’s maritime transportation system. The United Nations Conference on Trade and Development (UNCTAD) estimated in 2001 that 5.8 billion tons of goods were traded by sea in 2001; more than 80 percent of the world’s trade. This fact alone makes maritime networks an attractive target of terrorists. Although it has been some time since Osama bin Laden has been seen, it is ominous that in one of his last video appearances in October 2004 he confirmed that his agenda remained primarily economic. While terrorists have in the past targeted land or aviation assets, experts believe that this could soon change to include shipping, port, coastal facilities, and container/container yards are increasingly vulnerable because secondary emphasis has been placed on hardening these assets due to the urgent need to address threats to aviation facilities and transportation. Intelligence officials have identified cargo freighters they believe are controlled by Al Qaida, which could be used by the terrorist network or its affiliates to ferry operatives, explosive components, cash or commodities on the high seas. One example is a well-dressed middle-eastern man discovered by Italian police who had hidden himself in a cargo container destined for the U.S. He was equipped with a bed, toilet, water supply, satellite phone, laptop computer, cameras and maps. He also had security passes to various airports in the U.S.

#### Terrorists very likely and would most likely use container ships to smuggle weapons

Konkel, 2005, (Todd Konkel- professor Edmund A. Walsh School of Foreign Service, Georgetown University) “Container Security: Preventing a Nuclear Catastrophe”, International Policy Solutions, <http://irps.ucsd.edu/assets/004/5372.pdf>)

This nation faces a potentially greater threat, however, from a weapon of mass destruction (WMD) making its way into the U.S. in one of the thousands of cargo containers that enter this country every day. In June 2004, the House Subcommittee on Coast Guard and Maritime Transportation issued a memo reflecting this view: “Despite the importance of seaport security, perhaps no other mode of transportation is currently more vulnerable to future attacks than our Nation’s Marine Transportation System.”1 Although a future attack involving a chemical or biological WMD could have tragic consequences, a nuclear weapon, which could cause hundreds of thousands of deaths in an instant, presents the most concerning threat. In Nuclear Terrorism: The Ultimate Preventable Catastrophe, Harvard professor Graham Allison shares a brief but revealing excerpt from a private conversation that took place with former Secretary of Homeland Security Tom Ridge in February 2004. When asked what worried him most, Secretary Ridge replied with a single word: “nuclear.”2 Later in his book, Allison states that a nuclear weapon used by terrorists in an attack on the United States “is far more likely to arrive in a cargo container than on the tip of a missile.”3 The threat of a nuclear attack involving a seaborne container lies at the nexus of two critically important security issues: the availability of nuclear materials and the vulnerability of cargo containers. Although the U.S. government has taken a number of steps in the past few years to secure nuclear materials and improve the security of the 2 country’s ports, the threat of a nuclear weapon entering the United States undetected in a shipping container remains very real. Much additional work, including international standards for container security and expanded international cooperation to prevent the proliferation of nuclear materials, is necessary to prevent a catastrophe that could dwarf the tragedy of 9/11.

And, A port attack collapses global free trade – our internal link outweighs – 3 week timeframe
Flynn 03 (Stephen, Nat’l Sec Studies, “The Fragile state of container security,” testimony before the senate, March 20 <http://www.cfr.org/publication.html?id=5730>)

A year later I joined with former senators Warren Rudman and Gary Hart in preparing our report, “America: Still Unprepared—Still In Danger.” We observed that “nineteen men wielding box-cutters forced the United States to do to itself what no adversary could ever accomplish: a successful blockade of the U.S. economy. If a surprise terrorist attack were to happen tomorrow involving the sea, rail, or truck transportation systems that carry millions of tons of trade to the United States each day, the response would likely be the same—a self-imposed global embargo.” Based on that analysis, we identified as second of the six critical mandates that deserve the nation’s immediate attention: “Make trade security a global priority; the system for moving goods affordably and reliably around the world is ripe for exploitation and vulnerable to mass disruption by terrorists.” This is why the topic of today’s hearing is so important. The stakes are enormous. U.S. prosperity—and much of its power—relies on its ready access to global markets. Both the scale and pace at which goods move between markets has exploded in recent years thanks in no small part to the invention and proliferation of the intermodal container. These ubiquitous boxes—most come in the 40’x8’x8’ size—have transformed the transfer of cargo from a truck, train, and ship into the transportation equivalent of connecting Lego blocks. The result has been to increasingly diminish the role of distance for a supplier or a consumer as a constraint in the world marketplace. Ninety percent of the world’s freight now moves in a container. Companies like Wal-Mart and General Motors move up to 30 tons of merchandise or parts across the vast Pacific Ocean from Asia to the West Coast for about $1600. The transatlantic trip runs just over a $1000—which makes the postage stamp seem a bit overpriced. But the system that underpins the incredibly efficient, reliable, and affordable movement of global freight has one glaring shortcoming in the post-9-11 world—it was built without credible safeguards to prevent it from being exploited or targeted by terrorists and criminals. Prior to September 11, 2001, virtually anyone in the world could arrange with an international shipper or carrier to have an empty intermodal container delivered to their home or workplace. They then could load it with tons of material, declare in only the most general terms what the contents were, “seal” it with a 50-cent lead tag, and send it on its way to any city and town in the United States. The job of transportation providers was to move the box as expeditiously as possible. Exercising any care to ensure that the integrity of a container’s contents was not compromised may have been a commercial practice, but it was not a requirement. The responsibility for making sure that goods loaded in a box were legitimate and authorized was shouldered almost exclusively by the importing jurisdiction. But as the volume of containerized cargo grew exponentially, the number of agents assigned to police that cargo stayed flat or even declined among most trading nations. The rule of thumb in the inspection business is that it takes five agents three hours to conduct a thorough physical examination of a single full intermodal container. Last year nearly 20 million containers washed across America’s borders via a ship, train, and truck. Frontline agencies had only enough inspectors and equipment to examine between 1-2 percent of that cargo. Thus, for would-be terrorists, the global intermodal container system that is responsible for moving the overwhelming majority of the world’s freight satisfies the age-old criteria of opportunity and motive. “Opportunity” flows from (1) the almost complete absence of any security oversight in the loading and transporting of a box from its point of origin to its final destination, and (2) the fact that growing volume and velocity at which containers move around the planet create a daunting “needle-in-the-haystack” problem for inspectors. “Motive” is derived from the role that the container now plays in underpinning global supply chains and the likely response by the U.S. government to an attack involving a container. Based on statements by the key officials at U.S. Customs, the Transportation Security Administration, the U.S. Coast Guard, and the Department of Transportation, should a container be used as a “poor man’s missile,” the shipment of all containerized cargo into our ports and across our borders would be halted. As a consequence, a modest investment by a terrorist could yield billions of dollars in losses to the U.S. economy by shutting down—even temporarily—the system that moves “just-in-time” shipments of parts and goods. Given the current state of container security, it is hard to imagine how a post-event lock-down on container shipments could be either prevented or short-lived. One thing we should have learned from the 9-11 attacks involving passenger airliners, the follow-on anthrax attacks, and even last fall Washington sniper spree is that terrorist incidents pose a special challenge for public officials. In the case of most disasters, the reaction by the general public is almost always to assume the event is an isolated one. Even if the post-mortem provides evidence of a systemic vulnerability, it often takes a good deal of effort to mobilize a public policy response to redress it. But just the opposite happens in the event of a terrorist attack—especially one involving catastrophic consequences. When these attacks take place, the assumption by the general public is almost always to presume a general vulnerability unless there is proof to the contrary. Government officials have to confront head-on this loss of public confidence by marshalling evidence that they have a credible means to manage the risk highlighted by the terrorist incident. In the interim as recent events have shown, people will refuse to fly, open their mail, or even leave their homes. If a terrorist were to use a container as a weapon-delivery devise, the easiest choice would be high-explosives such as those used in the attack on the Murrah Federal Building in Oklahoma City. Some form of chemical weapon, perhaps even involving hazardous materials, is another likely scenario. A bio-weapon is a less attractive choice for a terrorist because of the challenge of dispersing the agent in a sufficiently concentrated form beyond the area where the explosive devise goes off. A “dirty bomb” is the more likely threat vs. a nuclear weapon, but all these scenarios are conceivable since the choice of a weapon would not be constrained by any security measures currently in place in our seaports or within the intermodal transportation industry. This is why a terrorist attack involving a cargo container could cause such profound economic disruption. An incident triggered by even a conventional weapon going off in a box could result in a substantial loss of life. In the immediate aftermath, the general public will want reassurance that one of the many other thousands of containers arriving on any given day will not pose a similar risk. The President of the United States, the Secretary of Homeland Security, and other keys officials responsible for the security of the nation would have to stand before a traumatized and likely skeptical American people and outline the measures they have in place to prevent another such attack. In the absence of a convincing security framework to manage the risk of another incident, the public would likely insist that all containerized cargo be stopped until adequate safeguards are in place. Even with the most focused effort, constructing that framework from scratch could take months—even years. Yet, within three weeks, the entire worldwide intermodal transportation industry would effectively be brought to its knees—as would much of the freight movements that make up international trade.

#### Protectionism causes war and bioterrorism

Pazner 8 (Michael J., Faculty – New York Institute of Finance, Financial Armageddon: Protect Your Future from Economic Collapse, p. 137-138)

The rise in isolationism and protectionism will bring about ever more heated arguments and dangerous confrontations over shared sources of oil, gas, and other key commodities as well as factors of production that must, out of necessity, be acquired from less-than-friendly nations. Whether involving raw materials used in strategic industries or basic necessities such as food, water, and energy, efforts to secure adequate supplies will take increasing precedence in a world where demand seems constantly out of kilter with supply. Disputes over the misuse, overuse, and pollution of the environment and natural resources will become more commonplace. Around the world, such tensions will give rise to full-scale military encounters, often with minimal provocation. In some instances, economic conditions will serve as a convenient pretext for conflicts that stem from cultural and religious differences. Alternatively, nations may look to divert attention away from domestic problems by channeling frustration and populist sentiment toward other countries and cultures. Enabled by cheap technology and the waning threat of American retribution, terrorist groups will likely boost the frequency and scale of their horrifying attacks, bringing the threat of random violence to a whole new level. Turbulent conditions will encourage aggressive saber rattling and interdictions by rogue nations running amok. Age-old clashes will also take on a new, more heated sense of urgency. China will likely assume an increasingly belligerent posture toward Taiwan, while Iran may embark on overt colonization of its neighbors in the Mideast. Israel, for its part, may look to draw a dwindling list of allies from around the world into a growing number of conflicts. Some observers, like John Mearsheimer, a political scientists at the University of Chicago, have even speculated that an “intense confrontation” between the United States and China is “inevitable” at some point. More than a few disputes will turn out to be almost wholly ideological. Growing cultural and religious differences will be transformed from wars of words to battles soaked in blood. Long-simmering resentments could also degenerate quickly, spurring the basest of human instincts and triggering genocidal acts. Terrorists employing biological or nuclear weapons will vie with conventional forces using jets, cruise missiles, and bunker-busting bombs to cause widespread destruction. Many will interpret stepped-up conflicts between Muslims and Western societies as the beginnings of a new world war.

#### Nuclear terrorism is an existential threat—it escalates to nuclear war with Russia and China

**Ayson 10** (Robert Ayson, Professor of Strategic Studies and Director of the Centre for Strategic Studies: New Zealand at the Victoria University of Wellington, 2010 (“After a Terrorist Nuclear Attack: Envisaging Catalytic Effects,” Studies in Conflict & Terrorism, Volume 33, Issue 7, July, Available Online to Subscribing Institutions via InformaWorld)

A terrorist nuclear attack, and even the use of nuclear weapons in response by the country attacked in the first place, would not necessarily represent the worst of the nuclear worlds imaginable. Indeed, there are reasons to wonder whether nuclear terrorism should ever be regarded as belonging in the category of truly existential threats. A contrast can be drawn here with the global catastrophe that would come from a massive nuclear exchange between two or more of the sovereign states that possess these weapons in significant numbers. Even the worst terrorism that the twenty-first century might bring would fade into insignificance alongside considerations of what a general nuclear war would have wrought in the Cold War period. And it must be admitted that as long as the major nuclear weapons states have hundreds and even thousands of nuclear weapons at their disposal, there is always the possibility of a truly awful nuclear exchange taking place precipitated entirely by state possessors themselves. But these two nuclear worlds—a non-state actor nuclear attack and a catastrophic interstate nuclear exchange—are not necessarily separable. It is just possible that some sort of terrorist attack, and especially an act of nuclear terrorism, could precipitate a chain of events leading to a massive exchange of nuclear weaponsbetween two or more of the states that possess them. In this context, today’s and tomorrow’s terrorist groups might assume the place allotted during the early Cold War years to new state possessors of small nuclear arsenals who were seen as raising the risks of a catalytic nuclear war between the superpowers started by third parties. These risks were considered in the late 1950s and early 1960s as concerns grew about nuclear proliferation, the so-called n+1 problem. It may require a considerable amount of imagination to depict an especially plausible situation where an act of nuclear terrorism could lead to such a massive inter-state nuclear war. For example, in the event of a terrorist nuclear attack on the United States, it might well be wondered just how Russia and/or China could plausibly be brought into the picture, not least because they seem unlikely to be fingered as the most obvious state sponsors or encouragers of terrorist groups. They would seem far too responsible to be involved in supporting that sort of terrorist behavior that could just as easily threaten them as well. Some possibilities, however remote, do suggest themselves. For example, how might the United States react if it was thought or discovered that the fissile material used in the act of nuclear terrorism had come from Russian stocks,40 and if for some reason Moscow denied any responsibility for nuclear laxity? The correct attribution of that nuclear material to a particular country might not be a case of science fiction given the observation by Michael May et al. that while the debris resulting from a nuclear explosion would be “spread over a wide area in tiny fragments, its radioactivity makes it detectable, identifiable and collectable, and a wealth of information can be obtained from its analysis: the efficiency of the explosion, the materials used and, most important … some indication of where the nuclear material came from.”41 Alternatively, if the act of nuclear terrorism came as a complete surprise, and American officials refused to believe that a terrorist group was fully responsible (or responsible at all) suspicion would shift immediately to state possessors. Ruling out Western ally countries like the United Kingdom and France, and probably Israel and India as well, authorities in Washington would be left with a very short list consisting of North Korea, perhaps Iran if its program continues, and possibly Pakistan. But at what stage would Russia and China be definitely ruled out in this high stakes game of nuclear Cluedo? In particular, if the act of nuclear terrorism occurred against a backdrop of existing tension in Washington’s relations with Russia and/or China, and at a time when threats had already been traded between these major powers, would officials and political leaders not be tempted to assume the worst? Of course, the chances of this occurring would only seem to increase if the United States was already involved in some sort of limited armed conflict with Russia and/or China, or if they were confronting each other from a distance in a proxy war, as unlikely as these developments may seem at the present time. The reverse might well apply too: should a nuclear terrorist attack occur in Russia or China during a period of heightened tension or even limited conflict with the United States, could Moscow and Beijing resist the pressures that might rise domestically to consider the United States as a possible perpetrator or encourager of the attack? Washington’s early response to a terrorist nuclear attack on its own soil might also raise the possibility of an unwanted (and nuclear aided) confrontation with Russia and/or China. For example, in the noise and confusion during the immediate aftermath of the terrorist nuclear attack, the U.S. president might be expected to place the country’s armed forces, including its nuclear arsenal, on a higher stage of alert. In such a tense environment, when careful planning runs up against the friction of reality, it is just possible that Moscow and/or China might mistakenly read this as a sign of U.S. intentions to use force (and possibly nuclear force) against them. In that situation, the temptations to preempt such actions might grow, although it must be admitted that **any** preemption would probably still meet with a devastating response. As part of its initial response to the act of nuclear terrorism (as discussed earlier)Washington might decide to order a significant conventional (or nuclear) retaliatory or disarming attack against the leadership of the terrorist group and/or states seen to support that group. Depending on the identity and especially the location of these targets, Russia and/or China might interpret such action as being far too close for their comfort, and potentially as an infringement on their spheres of influence and even on their sovereignty. One far-fetched but perhaps not impossible scenario might stem from a judgment in Washington that some of the main aiders and abetters of the terrorist action resided somewhere such as Chechnya, perhaps in connection with what Allison claims is the “Chechen insurgents’ … long-standing interest in all things nuclear.”42 American pressure on that part of the world would almost certainly raise alarms in Moscow that might require a degree of advanced consultation from Washington that the latter found itself unable or unwilling to provide. There is also the question of how other nuclear-armed states respond to the act of nuclear terrorism on another member of that special club. It could reasonably be expected that following a nuclear terrorist attack on the United States, both Russia and China would extend immediate sympathy and support to Washington and would work alongside the United States in the Security Council. But there is just a chance, albeit a slim one, where the support of Russia and/or China is less automatic in some cases than in others. For example, what would happen if the United States wished to discuss its right to retaliate against groups based in their territory? If, for some reason, Washington found the responses of Russia and China deeply underwhelming, (neither “for us or against us”) might it also suspect that they secretly were in cahoots with the group, increasing (again perhaps ever so slightly) the chances of a major exchange. If the terrorist group had some connections to groups in Russia and China, or existed in areas of the world over which Russia and China held sway, and if Washington felt that Moscow or Beijing were placing a curiously modest level of pressure on them, what conclusions might it then draw about their culpability? If Washington decided to use, or decided to threaten the use of, nuclear weapons, the responses of Russia and China would be crucial to the chances of avoiding a more serious nuclear exchange. They might surmise, for example, that while the act of nuclear terrorism was especially heinous and demanded a strong response, the response simply had to remain below the nuclear threshold. It would be one thing for a non-state actor to have broken the nuclear use taboo, but an entirely different thing for a state actor, and indeed the leading state in the international system, to do so. If Russia and China felt sufficiently strongly about that prospect, there is then the question of what options would lie open to them to dissuade the United States from such action: and as has been seen over the last several decades, the central dissuader of the use of nuclear weapons by states has been the threat of nuclear retaliation. If some readers find this simply too fanciful, and perhaps even offensive to contemplate, it may be informative to reverse the tables. Russia, which possesses an arsenal of thousands of nuclear warheads and that has been one of the two most important trustees of the non-use taboo, is subjected to an attack of nuclear terrorism. In response, Moscow places its nuclear forces very visibly on a higher state of alert and declares that it is considering the use of nuclear retaliation against the group and any of its state supporters. How would Washington view such a possibility? Would it really be keen to support Russia’s use of nuclear weapons, including outside Russia’s traditional sphere of influence? And if not, which seems quite plausible, what options would Washington have to communicate that displeasure? If China had been the victim of the nuclear terrorism and seemed likely to retaliate in kind, would the United States and Russia be happy to sit back and let this occur? In the charged atmosphere immediately after a nuclear terrorist attack, how would the attacked country respond to pressure from other major nuclear powers not to respond in kind? The phrase “how dare they tell us what to do” immediately springs to mind. Some might even go so far as to interpret this concern as a tacit form of sympathy or support for the terrorists. This might not help the chances of nuclear restraint.

#### Increasing the risk of detection deters terrorism

Konkel, 2005 (Todd, Professor Edmund A. Walsh School of Foreign Service, Georgetown University “Container Security: Preventing a Nuclear Catastrophe”, International Policy Solutions, http://irps.ucsd.edu/assets/004/5372.pdf)

This has created a situation where terrorists seeking to smuggle a nuclear weapon into the U.S. via a cargo container face highly favorable odds of escaping detection. According to one study, in fact, the probability that inspectors will detect a shielded nuclear weapon in a shipping container using the current screening system is only about 10 percent.27 In order to decrease the likelihood of a nuclear weapon entering the U.S. in a container, the odds of detection must be significantly improved. Otherwise, terrorists will eventually attempt to exploit this system, given the relatively low risk that a nuclear weapon or dirty bomb would be detected.

#### Contention 2 is solvency

#### And the USFG is key - states require the federal government for effective port upgrades because of interstate competition and a failure to share solutions

Puentes 5/23/2011 (Robert Puentes, Senior Fellow and director of Metropolitan Policy at Brookings, former Director of Infrastructure at the Intelligent Transportation Society of America, “Move It: How the U.S. Can Improve Transportation Policy”; http://www.brookings.edu-/research/opinions/2011/05/23transportation-policy-puentes)

The country needs to become more export-oriented for the future health of the economy. But right now there's no way to make sure that the nation's ports, border crossings and roadways are set up to accomplish that goal. For one thing, there's far too little attention paid to making sure that traffic at border crossings moves swiftly. Our crossings into Mexico and Canada are routinely clogged, interrupting the flow of trade. Consider the challenges facing Detroit—part of the largest binational trading corridor on the planet, linking the U.S. and Canadian auto industries and other sectors with highly integrated, transport-dependent, "just in time" supply chains and their smaller, more frequent shipments. Canada is our nation's largest trading partner, and Detroit's Ambassador Bridge is the No. 1 border point for commerce between the two countries. It's a crucial corridor—but there are relatively few border crossings because of the Great Lakes. So traffic piles up at bridges and tunnels, with freight competing with passenger cars to get through tightened security checkpoints. Trucks also clog the roads of Detroit as they shuttle freight between ports and large distribution centers and warehouses. The export problem isn't just a matter of insufficient infrastructure. States and cities routinely compete against one another for shipping activity instead of coming up with joint efforts that might benefit all the terminals in the region. Without an overall strategy, there's a duplication of efforts and a duplication of subsidies that hurts the economy, given scarce resources. Collaboration is needed—between the federal government, states, metro areas, freight industry and shippers. We need to come up with a comprehensive plan that identifies the best ways to help the flow of freight. The plan might identify the most important corridors for freight, for instance, and then target investments to improve safety, relieve bottlenecks and provide better access to ports. That might mean new roads leading to ports or, in some instances, truck-only lanes on existing roads. Similarly, the U.S., Canada, and Mexico should also come together to study infrastructure needs at the land borders and along the corridors that link the two borders together. For now, some states are coming up with innovative solutions on their own—solutions that could and should become widespread under a national transportation policy. Back in Detroit, for instance, the national governments of the U.S. and Canada, along with lawmakers in Michigan and Ontario, are trying to build a new bridge across the Detroit River to help keep trade flowing—a plan that's awaiting final legislative approval. Meanwhile, the World Trade Bridge in Laredo, Texas, has introduced tags for electronic toll collection to speed traffic and reduce wait times. Then, of course, there's the issue of competition between ports for shipping business. One way to ease that problem: Tell states their ports won't get any federal aid unless they work with their neighbors to boost business in the whole region. And those agreements need to be carefully structured and policed to make sure they don't collapse—which happens all too easily. Consider the current mess involving Jasper Ocean Terminal on the Savannah River, the border between South Carolina and Georgia. In 2007, the two states agreed to develop the terminal together, and create a special entity to own and operate it. That's good. But what came later wasn't. After the governors who signed the deal left office, the terminal became a point of contention between the states. What happened? Georgia decided it wanted to deepen another one of its own harbors, a move that South Carolina sees as a challenge to its own facilities. So, South Carolina has stopped funding the Jasper facility unless the Georgia dredging plan is scrapped. Now, I ask you: How does any of this help get us closer to our national goals?

#### Risk management principles are key—funding allocation and Port Security Grant Program eligibility

GAO, 11/11/2011 (“PORT SECURITY GRANT PROGRAM: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened” United States Government Accountability Office http://www.gao.gov/products/GAO-12-47)

In recent years, we, the Congress, the President, the Secretary of Practices Associated with Homeland Security, and others have endorsed risk management as a way to direct finite resources to areas that are most at risk of terrorist attack. Risk management is a continuous process that includes the assessment of threats, vulnerabilities, and consequences to determine what actions should be taken to reduce one or more of these elements of risk. One way in which DHS has applied risk management principles to the PSGP is through the use of a risk model to assess the relative risk posed to ports throughout the nation and to help determine PSGP eligibility and funding levels. The PSGP risk methodology is similar to the methodology used to determine funding eligibility for other DHS state and local grant programs. The model consists of three variables: threat (the relative likelihood of an attack occurring), vulnerability (the relative exposure to an attack), and consequence (the relative expected impact of an attack). Data for each of these variables are collected from offices and components throughout DHS, as well as from other data sources, and then, using the model, each port is ranked against one another and assigned a relative risk score. At the recommendation of the Coast Guard, DHS considers some ports as a single cluster—known as a port area—due to geographic proximity, shared risk, and a common waterway. Based on risk, each port area is placed into one of three funding groups— Group I, Group II, or Group III.11 Ports not identified in Group I, II, or III are eligible to apply for funding as part of the “All Other Port Areas” Group.12 Figure 2 below shows the location of port areas for groups I and II—the two highest risk groups that receive the bulk of grant funding.

#### GAO reforms key to solve delays

GAO, 11/11/2011 (“PORT SECURITY GRANT PROGRAM: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened” United States Government Accountability Office http://www.gao.gov/products/GAO-12-47)

Port areas have unique characteristics—they are centers of commerce, hubs of transportation, and often close to major population centers. These characteristics result in specific vulnerabilities that must be addressed to avoid the human or economic losses that would result from a terrorist attack. The Port Security Grant Program (PSGP)—administered by FEMA and supported with subject matter expertise from the Coast Guard—is one tool DHS uses to protect critical maritime infrastructure from these risks. Risk management has been endorsed by the federal government to help direct finite resources to areas of greatest risk and grant programs have provided substantial resources toward this effort. We found that PSGP allocations were highly correlated to risk for the grant years we examined and DHS has taken steps to strengthen the PSGP risk allocation model by improving the quality and precision of the data inputs. However, additional efforts—such as accounting for how new security measures affect port vulnerability and using the most precise data available in the risk model—could further strengthen the model and build upon the progress made. While the allocation process has been riskbased, FEMA has faced significant challenges administering the grant program. For example, FEMA awarded nearly $1.7 billion in port security grants for fiscal years 2006 through 2010; however, draw down levels for the PSGP are low—with about one-quarter of fiscal year 2006 through 2010 grant monies drawn down as of September 2011. While FEMA may not consider draw down levels to be an accurate measure of progress made in improving port security, this measure has become the de facto yardstick for assessing progress in securing our ports because no other measures exist. Additionally, about a quarter of the awarded funding remains unavailable due to delays in using grant funds, challenges with the cost-match and associated waiver process, and challenges that grantees have had complying with postaward requirements. As a result, about $400 million in awarded grant funding remains unavailable to grantees for port security projects. FEMA has taken steps to improve the availability of funds and has developed internal performance measures to begin evaluating its administration of the grant program. However, FEMA has not evaluated the effectiveness of the program because it does not have measures to track progress towards achieving program goals. To establish a more accurate measurement of grant effectiveness, FEMA should expedite its efforts to implement performance measures for the PSGP. Initial steps have been taken to develop performance measures for the PSGP, but the time frame for implementing them is unclear. Without a plan, there is little assurance that these measures will be implemented in a timely way to assess the program’s effectiveness in ensuring that critical port infrastructure is protected.

## Affirmative

### Inherency/Uniqueness

#### C-TPAT Fails

#### C-TPAT is unable to perform its duties and carry out its goals

John J. O’Connell 09, Journal of Transportation securityhttp://www.springerlink.com/content/78317530844937h2/ C-TPAT: Major Challenges

Since its implementation after the 9/11 attack on the World Trade Center, the Customs Trade Partnership Against Terrorism (C-TPAT) has grown to be one of the largest public/private partnerships in the world. The focus of C-TPAT is on the United States’ vulnerability to the smuggling of weapons of mass destruction (WMD) across its borders. As a system, C-TPAT has achieved great success; however, there remain a number of serious deficiencies that C-TPAT, by itself, cannot overcome. Very few cargo containers are currently being inspected by Customs and Border Protection (CBP). This is due to lack of funding and manpower deficiencies as well as the practical need to allow the flow of trade to continue as swiftly as possible. Instead of mass inspection of containers, CBP relies on its ability to identify and further question or inspect “high risk” containers before they are shipped or prior to their entry to the United States. Identifying “high risk” containers results in a far lower number of CBP inspections, thereby offering less interference with the trade process. It is well known amongst shipping experts that the contents of many containers are mislabeled or misdeclared. Combine the fact that many cargo containers contain misdeclared contents with the current model of inspecting very few containers and one can conclude that the potential for problems is enormous. Furthermore, concerns over specificity of standards related to C-TPAT security requirements and the likelihood that membership in C-TPAT increases an organization’s potential for attack and the situation continues to deteriorate. C-TPAT began as and remains an initiative with honorable goals; however, we cannot rely upon increasing numbers of C-TPAT members as a measure of its effectiveness.

#### C-TPAT has four major problems associated with it

John J. O’Connell 09, Journal of Transportation securityhttp://www.springerlink.com/content/78317530844937h2/ C-TPAT: Major Challenges

Many problems are related to lack of funding of CBP which results in inadequate numbers of inspectors or agents as well as other administrative needs of the program. Although additional problems exist, the author has elected to review four potentially serious problems related to the functioning of the C-TPAT program itself for which support is found in the recent literature. For a review of problems identified by the United States Governmental Accountability Office (GOA) see the GOA 2005 and 2008 reports. 7 The problems reviewed are: 1. Membership in C-TPAT May Increase the Threat to that Member’s Supply Chain 2. C-TPAT Lacks Specificity as to Required Security Standards 3. Few Containers are Being Inspected by CBP 4. Mislabeled Cargo or Insufficient Information on Cargo Manifests Each area taken individually is sufficiently problematic to warrant review and repair as soon as possible. When taken as an interrelated set of problems, however, they become truly momentous.

#### Few Containers are being inspected by the CBP

John J. O’Connell 09, Journal of Transportation securityhttp://www.springerlink.com/content/78317530844937h2/ C-TPAT: Major Challenges

The number of actual physical inspections is one area of concern in which there is little dissention by any party. In order to show the importance of the area of concern, let us assume that approximately 10 million containers are expected to enter the United States by sea in 2009; “Currently, approximately 5% of incoming containers from the sea are selected for additional scrutiny, which consists of a two stage inspection process…. Primary inspection consists of scanning via an x-ray or a gamma-ray scanner. Inspectors examine the scanned image for discrepancies with the manifest and other signs of risk.” The second step, if necessary is an “actual physical inspection. …it is estimated that roughly 5 per cent …are selected for additional scrutiny” 12 Based upon current estimates, if 10 million containers crossed our borders, 500,000 would be subjected to scanning and 25,000 would be scheduled for actual physical inspection or about 2.5 per 1000. It should be noted that an external inspection in the form of scanning for radiological content now takes place in many foreign ports and is not included in the above estimates. Thus, for at least the nuclear exposure the number of scanned (partially inspected) containers is far more then the 5% quoted above. The number of uninspected containers is a serious deficiency in C-TPAT and one of the reasons why the WMD exposure from imported containers is so high. The number of containers inspected, however, may be deceiving. The CBP justifies the relatively small number of containers inspected by pointing to its investigative 11 Op cit, Brandman. 12 “Evaluating the Viability of 100 Per Cent Container Inspection at America’s Ports”; By: Martonosi et al. 2005. C-TPAT: major challenges 143efforts to identify high risk containers. Further, under another CBP program, the Container Security Initiative (CSI), CBP enlists the formal assistance of foreign port operators to identify and inspect high risk containers before they are loaded onto vessels for shipment to the U.S. As of 2008 CSI had agreements with 35 Customs administrations covering 58 foreign ports and approximately 86% of U.S. bound containers.

#### Containers aren’t inspected thoroughly enough by the CBP

John J. O’Connell 09, Journal of Transportation securityhttp://www.springerlink.com/content/78317530844937h2/ C-TPAT: Major Challenges

Identifying high-risk containers is the mainstay of the C-TPAT and the Container Security Initiative (CSI) and the basis of CBP’s system to select containers on which to secure additional review of shipping papers or to hold for additional inspections. As outlined in problem 3 above, one of the basic problems associated with any program to secure container cargo from tampering or the introduction of various forms of contraband is that it would be very rare for “any” authority (governmental or other) to actually thoroughly inspect the contents of the container itself. This significant drawback applies to the C-TPAT program as well and is unlikely to be cured in the foreseeable future. High-risk containers are identified partially by reviewing the cargo manifests of containers bound for the United States. All else being equal the cargo manifest is assumed to accurately describe not only the types of cargo being transported but other information such as the names of the parties involved and origination and delivery points. This assumption, however, may be far from true. A number of studies have found that misdeclaration of contents of containers or other documentation errors are a major problem in the shipping industry. James McNamara, President of the National Cargo Bureau, Inc., indicated in a presentation to the International Union of Maritime Insurers stated that misdeclaration by shippers is a major problem and without full inspection these misdeclared containers would be distributed without much problem (Kimery 2008). In his article on misdeclared ship cargo Anthony Kimery stated: “US maritime, customs and counter terror officials told HSToday on background they agree with McNamara, who pointed to the disturbing findings of a yearlong audit of containers conducted by seven nations for the IMO. The survey concluded in August 2006.

#### CSI Fails

#### The Container Security Initiative is, as of now, a failure.Lofgren (Zoe Lofgren, Congresswoman representing California’s 16th District, “Statement of Congresswoman Lofgren on 9/11 Resolution”)

[lofgren.house.gov/index.php?option=com\_content&view=article&id=155&Itemid=130](http://lofgren.house.gov/index.php?option=com_content&view=article&id=155&Itemid=130)

Congresswoman Zoe Lofgren (D-CA) today submitted the following statement, “Yes, the Administration has finally ‘initiated . . . the Container Security Initiative, to extend our borders overseas and to secure and screen cargo before it is placed on ships destined for United State ports of entry.’ However, initiation of a program is a far cry from fully administering the program and contributing to our homeland security.  The Container Security Initiative is, so far, a failure.  “The resolution gives us the false impression that the US-VISIT border security screening system is fully operational and ensuring our homeland security.  Yet, the Administration has not even connected US-VISIT port of entry systems to a central database that can handle immediate screenings upon entry.”

#### Ports Vulnerable

**Less than 3% of containers scanned now- creates major security risk**

Hahn 12 (Congresswoman Janice Hahn, Congressional Documents and Publications, May 9, 2012, “Congresswoman [Laura Richardson](http://w3.nexis.com/new/search/XMLCrossLinkSearch.do?bct=A&risb=21_T14683658970&returnToId=20_T14683673387&csi=247474&A=0.13662523131856086&sourceCSI=162599&indexTerm=%23PE000A0V6%23&searchTerm=Laura%20Richardson%20&indexType=P) Asks GAO to Examine Port Security Vulnerabilities”; Rep. [Laura Richardson](http://w3.nexis.com/new/search/XMLCrossLinkSearch.do?bct=A&risb=21_T14683658970&returnToId=20_T14683673387&csi=247474&A=0.13662523131856086&sourceCSI=162599&indexTerm=%23PE000A0V6%23&searchTerm=Laura%20Richardson%20&indexType=P) (D-CA) News Release, <http://richardson.house.gov/index.php?option=com_content&view=article&id=2948&Itemid=500261>)

Congresswoman Janice Hahn’s bill, H.R. 4005 “Gauging American Port Security Act” or Gaps Act, today successfully passed by a unanimous vote in the Homeland Security Committee. H.R. 4005 directs the Department of Homeland Security to conduct a comprehensive classified examination of remaining gaps in port Security and prepare a plan to address them. “Pretending a threat doesn’t exist does not make it go away,” Rep. Hahn said. “The lesson of 9/11 is to be vigilant and proactive in seeking out and preventing our country’s most pressing threats. More than a decade after 9/11, our ports remain possible points of entry for terrorists and their weapons. Ports are also a key part of our economy. If an attack were ever to occur, it would cause a catastrophic loss of jobs and damage to our economic recovery. This situation requires a legislative solution and I hope that the resulting blueprint will guide Congress in creating effective legislation to help guard our ports.” Ships make 50,000 calls a year on U.S. ports, carrying two billion tons of freight and 134 million passengers. Each day our ports move both imports and exports totaling some $3.8 billion worth of goods through all 50 states. Additionally, ports move 99.4 percent of overseas cargo volume by weight and generate $3.95 trillion in international trade. Unfortunately less than 3% of cargo coming into the country is scanned, giving terrorist opportunities to smuggle themselves or their weapons into the United States with little risk of detection. An attack on the Port of Los Angeles complex, for example, would cost billions to the regional economy and put thousands of port employees out of work and cause the demise of hundreds of local businesses.

#### Current efforts to deter dangerous materials from being shipped are failing

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

#### Port Security not good right now

Maritime Security Review, 2/22 **(Mark Lowe, “Cargo Vulnerable to terrorist”, Maritime Security Review,** [**http://www.marsecreview.com/2012/02/cargo-vulnerable-to-terrorists/**](http://www.marsecreview.com/2012/02/cargo-vulnerable-to-terrorists/)**)**

A decade after The Maritime Transportation Security Act (MTSA) of 2002 was introduced, a new US Government report has criticised efforts to protect global supply chains. U.S. bound cargo remains vulnerable to terrorists It’s been more than a decade since Islamic terrorists attacked the U.S., yet the agency created to protect the nation from another strike is asleep at the wheel, failing to adequately screen the monstrous amounts of cargo that enter the country each day, according to a government report issued this week. “Cargo containers that are part of the global supply chain — the flow of goods from manufacturers to retailers — are vulnerable to threats from terrorists [including weapons of mass destruction],” state the government analysts who assembled data for the new report. It may seem unbelievable to most Americans that the Department of Homeland Security (DHS) that more than ten years after the worst terrorist attack in U.S. history, the vast majority of cargo containers entering the U.S. go unchecked. Incredibly, it’s true and the alarming details are outlined in the GAO report published this week by the Government Accountability Office (GAO), the investigative arm of the U.S. Congress. The Maritime Transportation Security Act (MTSA) of 2002 and the Security and Accountability For Every (SAFE) Port Act of 2006 required the

Large security gaps in ports.

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)

Port security, however, is not a unilateral endeavor. It involves all levels of government, private domestic and international businesses, and foreign governments. Also, it encompasses numerous issues— from the security of actual port facilities to passenger identity verification to threats posed by container cargo shipments. Prior to post-9/11 initiatives, nowhere were the gaps in security more startling than in the importation of cargo packaged in shipping containers. Shipping containers travel the seas and enter ports with seeming anonymity and little verification of their contents. Though a particular port “may accommodate anything from recreational watercraft, to barges, ferries, and ocean-going cargo and passenger ships,” 1 many ports along the southeastern United States tend to operate predominantly as cargo ports and are large contributors to the global supply chain. Given the robust container ports in the southeastern United States, including North and South Carolina, changes in container security measures are of great concern in these communities.

#### Shipping Increasing

#### Use of shipping containers is increasing.

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)

Some of these ports may not handle large quantities of cargo or may handle bulk cargo but not cargo carried in containers. What is clear is that the volume of those ports welcoming container shipments will continue to increase. Between 2001 and 2020, international container shipments are expected to double. 29 Though presumably good news for world trade, the increase in container shipments also mandates the need for efficient and effective methods of screening containers.

#### Worldwide funding for port security is not keeping up with Demand

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)

In spite of awareness by public policymakers that ports remain critically vulnerable 3 , funding and government-led efforts to harden port facilities worldwide is moving at a glacial pace. Terrorists, in particular, are aware of this unaddressed vulnerability. As outlined below, the threats to the maritime industry are very real. Unfortunately, the question of whether terrorists will act to exploit the weaknesses in port facilities is, unfortunately, not a matter of “if” they will, but “when” they will.

#### Though many actions have attempted to reduce terrorist attacks, they still manage to train and are ready for the small port security available. Funding necessary.

WI-LTD n.d.-n.d.-’09 (Westminster Ltd., British security company providing service in over 45 countries, “Ports and Harbour Security”, WI-ltd., <http://www.wi-ltd.com/Solutions_by_Sector/Ports_and_Harbours>)

The massive growth of shipping around the world and the globalisation of the container business has brought its own security problems and increased threats to Ports and Harbours worldwide. The International Maritime Organisation (IMO) issued the International Ship and Port Facility Security (ISPS) Code as an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies with an effective date of 2004. The Code is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. All international Ports and Harbours are required to implement the Code. The threat of terrorist attack on naval bases, harbours, ports, oil platforms, terminals, underwater pipelines, shipping and coastal facilities remains a real and growing concern to all countries. Terrorist organisations are now training operatives in diving techniques, and the risk of attack on facilities from diver teams is now very real.

#### Grants Not Funded

#### Current grants don’t solve port security

Redfern 12-1-10 (Jocelyn Redfern, Maritime Publishing, BA Religious Studies from McGill University; “Port Security: Good News, Bad News, No News at All”; MaritimeProfessional; http://maritimeprofessional.com/Blogs/The-Final-Word-with-Joseph-Keefe/December-2010/Port-Security--Good-News,-Bad-News,-No-News-at-All.aspx)

In simple terms, the cost-share requirement (for ports, local entities, states) is a drag on the ability of ports to move forward with projects to improve security, based on federal port security grant rules. As a result, only about $21 million of the $755 million in awarded funds for fiscal years 2006 through 2008 had been expended by transit agencies. And, while GAO says that they are, this month initiating a review of grant management processes of selected DHS preparedness grant programs, the requirement that local entities share in the cost of security projects that benefit individual ports – in my opinion – is a good one. First, it shows stakeholder buy-in and secondly, it provides a reasonable assurance that the funds will be spent and utilized correctly on the local level. Those local entities cannot get their act together to properly submit paperwork should not be the problem of DHS, but on the other hand, port security issues remain unsolved in the balance. What’s a mother to do?

### Economy Adv.

#### Key to Competitiveness

#### Port security is key to economic competitiveness

Paul Barnes Richard Oloruntoba 04 Queensland University of Technology, School of International Business, Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management, http://www.sciencedirect.com/science/article/pii/S1075425305000694

Effective and efficient systems of transportation are critical to domestic and international business. Along with trade liberalization, the adoption of international standards, advanced telecommunications and the capacity to transport goods and commodities are critical factors in globalized and interdependent economies (Kumar and Hoffmann, 2002). In addition, effective and efficient systems of transportation are critical to optimizing transport and transaction costs and global competitiveness generally.A study by the World Bank found that increased port efficiency has a significant and positive impact on the expansion of trade, as are improvements in the customs regulatory environment. Wilson et al. (2003) argue that burdensome customs and regulatory/security measures may hinder port and maritime supply chain efficiency, which in turn leads to a contraction in trade and overall efficiency. While the notion of a competitive company is clear, the notion of a competitive nation is not. Ultimately, the source of competitive advantage rests at the industry level and regional level. Studies examining the factors that confer advantage to particular industry sectors have sought ideal policy positions that governments might pursue to generate a competitive edge for domestic industries ( [Garelli, 2001] and [Farrugia, 2002]). The International Institute for Management Development considers aspects of structural factors affecting long term economic performance as encapsulated in the concept of competitiveness with respect to productivity, skills and innovation in an economy (Fagerberg, 1996). Not-with-standing notions of global competitiveness, the focus of this article is on regional competitiveness. This makes considerable sense in that any loss of competitiveness in trade will impact directly on regional economies especially those with a higher than average density of trade-related infrastructure that would normally be found adjacent to ports and surrounding hinterlands. An economic impact study carried out by the St Lawrence Seaway Development Corporation (SLSDC) in 2001 highlights how the presence of an efficient maritime trading system can enhance regional competitiveness. The study included the St. Lawrence Seaway and related waterways, ports and their inter-modal connections, as well as vessels, vehicles and other system users. The SLSDC report indicated a total of 152,508 jobs are in some way related to the 192 million tonnes of cargo moving on the US side of the great lakes seaway system in 2000 (U.S. Dept. of Transportation, 2002).

### Terrorism Adv.

#### Terrorism Likely

#### Sea ports are vulnerable but the US has not funded enough

Konkel, Comstock Spring 2005 (Todd Konkel, @ the Edmund A. Walsh School of Foreign Service, Georgetown University, Container Security: Preventing a Nuclear Catastrophe, IPS, <http://irps.ucsd.edu/assets/004/5372.pdf>)

According to Stephen Flynn, a Senior Fellow in National Security Studies at the Council on Foreign Relations, the CIA has concluded that the most likely way that a WMD would enter the U.S. is by sea. 28 Despite this assessment, as of September 2004, the U.S. government was spending more every three days to finance the war in Iraq than it had provided over the previous three years to improve security at all 361 U.S. seaports. 29 9 Container Security: Preventing a Nuclear Catastrophe Todd Konkel V. Current Initiatives Preventing terrorists from smuggling a nuclear weapon into the country in a shipping container will require concurrent efforts both to reduce the availability of nuclear materials and to improve the security of maritime cargo transportation. The U.S. government has launched several programs to tackle each of these issues, but these existing initiatives fall short of what is necessary to achieve adequate security.

#### Ports are vulnerable to weapons and terrorist entry.

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 security weaknesses surrounding shipping containers are not typically the first concern when considering overall port security. For example, when news first broke that Dubai Ports World— through its purchase of Peninsular and Oriental Steam Navigation Company, a company already leasing marine terminals around the world, including five United States ports— may take over operation of several marine terminals in this country, 3 many appeared to assume security would be newly threatened by the involvement of foreign entities in port operations. 4 As will become apparent, not only are foreign entities already heavily invested in United States port operations, but the cooperation of private and governmental interests in other countries is crucial to securing, among other things, container shipments into United States ports. Rather than foreign investment, the real security issue surrounding shipping containers is the anonymity of those involved with the shipment and of the cargo actually contained inside. Regardless of any opposition to marine terminal or other port facility operations, “ports are vulnerable to the entry of terrorists or illicit weapons because of the large number of containers that enter U.S. territory, regardless of who manages them.” 5

#### Ports are vulnerable to terrorists – Multiple warrants.

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 rise of shipping containers, though beneficial to world trade and globalization, also creates security concerns. These concerns stem from the limited scrutiny at ports of arriving cargo, the large volume of containerized cargo arriving at ports around the world, and the very fact that closed containers do not lend themselves to easy or economically efficient inspection. In 2005, Senator Carl Levin of Michigan referred to ports as a modern day “Trojan horse.” 13 Other government officials voiced similar concerns for the perceived holes in overall port security. 14 Maritime experts had been warning of the “Trojan Horse” style threat of shipping containers as well. 15 Indeed, many quickly concentrated on the unique risks posed by container shipments, shipping containers having also been characterized as a potential “poor man’s missile.” 16 The use of containers in the global supply chain involves a complex network of manufacturers, exporters, importers, brokers, carriers and foreign customs and port officials. What ultimately arrives in a shipping container shipped to a United States port depends on the actions and information provided by these numerous entities and individuals. Everyone from manufacturers to land carriers to middlemen freight forwarders to customs brokers, terminal operators and port employees (including management, stevedores, and longshoremen) at every port entered by the carrying vessel play a role in securing the cargo and the locations to which it is sent. 17 The many hands that access a single container create a number of significant container security issues. Opportunities for security breaches occur primarily in the following stages of the shipping process: (1) the packing process at the foreign warehouse or factory; (2) the transport of the packed goods from that location to the foreign port at which the goods will be loaded; and (3) the preparation of the cargo manifest setting forth the contents and other information about the goods being shipped. 18 Given these opportunities to tamper with the shipment process, container security efforts focus in large part on container inspection and documentation, container seals, and the secure storage of containers. The many steps in the shipment of goods via shipping container from manufacturer to end consumer provide opportunities for tampering to petty criminals and terrorists alike. Unfortunately, the risks with which ports and customs officials remain most familiar are those associated with normal criminal activity, not terrorism. Efforts that effectively address traditional criminal concerns, such as drug smuggling and human trafficking, may not aid in identifying containers posing a high risk of terrorist use. “[W]hat may have made sense for combating crime does not automatically translate to combating determined terrorists.” 19 Indeed, at least three distinctions exist between basic criminal activity and the likely actions of terrorists: (1) most security measures focus on identifying criminal patterns and behaviors in order to identify high risk shipments, whereas would-be terrorists are typically engaged in one-time operations; (2) rather than avoiding legitimate channels of trade to evade detection of ongoing criminal activity, terrorists have no reason not to use, and likely would prefer to use, legitimate companies and methods of shipment into the United States banking on such shipments being subjected to little or no inspection; and (3) traditional criminal use of legitimate companies and shipping avenues would result in unwanted attention and inspection of future smuggling shipments, whereas the use of such trusted shipments by terrorists furthers their goal of economic disruption. 20

#### Risk of Port terrorism is high – Past attempts and motive prove.

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)

Analysis of the ways in which terrorists may use container shipments is not based on mere hypothesis. On October 18, 2001, a stowaway was discovered within a shipping container ultimately bound for Canada. 42 The stowaway was discovered while the container was at the Italian port of Gioia Tauro. 43 This “stowaway,” Rizik Amid Farid, was a suspected Al Qaeda member and an Egyptian national. 44 He was traveling in a container that was outfitted with a bed, a heater, toilet facilities and water. 45 More disturbing were the items he carried with him; a Canadian passport, phones, a computer, airport security passes and an airline mechanic’s certificate that would enable him entry into sensitive areas at airports in New York, Chicago and Los Angeles. 46 Soon after his arraignment and release on bond, Farid disappeared. 47 Moreover, entire vessels are actually controlled by Al Qaeda. This terrorist organization may use those vessels for legitimate trade to raise funds or to carry out further terrorist activities. 48 The ease with which Farid clearly used a container for his own transport— only discovered when he attempted to widen ventilation holes with port employees nearby— is disturbing. 49 This successful concealment of container contents, along with potential Al Qaeda control of entire vessels able to carry thousands of shipping containers, is particularly troubling when the total volume of maritime container shipments in need of security screening is considered. “More than 80 percent of the world’s trade travels by water and forges a global maritime link. About half the world’s trade by value, and 90 percent of the general cargo, are transported in containers.” 50 Large volumes of trade via container shipments are processed through ports. Those ports also provide economic benefits to the surrounding communities. 51 Thus, threats by terrorists may have several objectives, including human casualties, environmental damage or economic loss and disruption. 52

#### High risk of terrorist attack on US Seaports

Lane, Colonel US Army 2/4/2009 (Drefus Sr. “U.S. SEAPORT SECURITY: CRITICAL CHALLENGE FOR DEPARTMENT OF HOMELAND SECURITY” USAWC STRATEGY RESEARCH PROJECT <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA499287>)

Vulnerabilities Pose Security Risks. There are various physical and infrastructural dimensions amongst seaports throughout the United States however; several have similar designs which cause them to be at risk to terrorist attacks. 8 These characteristics are relevant to both their framework and structure. These approaches make securing such expansive areas of entry even more complex when implementing security measures. Ports located in large industrial areas make it hard to execute the required security measures. Ports are largely located in urban areas where commercial activities involving fuel resources, storage and handling of hazardous products and materials are key components of the infrastructure. The dynamics of these arrangements are compounded because of the close location to bridges, railroads and industrial facilities. In addition, maintaining the ingress and egress of materials in these locations is of critical importance to the security and financial stability of the economies in this environment. Again facts such as these make the infrastructure, land and ports prime targets for illegal and terrorist activities. 9

#### Solvency - Must Increase Chance of Failure

#### **Terrorists deterred by failure – resources needed**

Vesky, 2008 (Jonathon P. Vesky, author of Port and Maritime Security, “Port and Maritime Security: Concerns for Port Security,” DOA: June 22, 2012)

What Priority Should Port Security Have?The 9/11 Commission wrote, “Opportunities to do harm are as great, or greater, in maritime or surface transportation [compared to commercial aviation]. Initiatives to secure shipping containers have just begun.” Terrorists “may be deterred by a significant chance of failure.” Improving the ability to detect terrorist nuclear weapons in the maritime transportation system may make a terrorist attack on a port less likely to succeed, and thus less probable. The American Association of Port Authorities, a trade association, welcomed federal grants for port security upgrades to comply with the MTSA, but called for “ substantially greater resources.” Others agree that more resources are needed to secure US ports, such as to reduce overcrowding of cargo-handling facilities and to hire more workers.” A similar case could be made for gas pipelines, electric power plants, rail yards, or bridges. At issue for Congress is how to allocate security funds among ports and other potential targets.

#### Improving detection is key to deter terrorism and reduce fraud.

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)

Prior to the terrorist attacks of September 11, 2001, the primary focus of port security was to prevent theft and to ensure that illegal or undeclared goods were not brought into the United States. The United States and international responses to the terrorist threat have expanded the focus of port security. Scanning equipment has enhanced security by enabling the detection of weapons at ports of entry, thereby preventing their transport onto the mainland by truck or train (Haverman & Shatz, 2006). Martonosi, Ortiz and Willis (2006) explain that complete scanning and subsequent inspection of containers at ports would most likely deter terrorists and smugglers under particular circumstances (see Table 1: Cargo scan location consequence matrix). A sufficiently high detection rate would render irrational an attempt to employ a container in an attack on an interior target, since it would have little chance of reaching the desired location (p.22). Haveman and Shatz (2006) further explain: “the burden thus falls on technology - on the intelligent deployment of existing technologies and the rapid development of new and better technologies. Used in conjunction with one another, rather than as replacements for one another, they could provide an excellent, although regrettably still imperfect, security shield (p.121).” The transformation of ships into floating warehouses, a consequence of just-in-time manufacturing strategies, combined with the digital transformation of supply chain management, has also rendered economies more vulnerable to terrorist disruption (Stowsky, 2005). Due to the impact of technology deployment on logistics and the international supply chain, the expectation is that better screening technologies will also reduce commercial losses from fraud by enabling the quicker detection of illegal or dangerous goods and their removal from the supply chain (Haveman & Shatz, 2006).

#### Protectionism Impacts

#### Protectionism makes political rivalries and conflict inevitable – empirics all go aff

Stewart Patrick, CFR International Institutions Director and Senior Fellow, 3/13/2009, "Protecting Free Trade," http://www.nationalinterest.org/Article.aspx?id=21084

President Obama has committed to working with U.S. trade partners to avoid “escalating protectionism.” He is wise to do so. As never before, U.S. national security requires a commitment to open trade. President Obama and his foreign counterparts should reflect on the lessons of the 1930s—and the insights of Cordell Hull. The longest-serving secretary of state in American history (1933–1944), Hull helped guide the United States through the Depression and World War II. He also understood a fundamental truth: “When goods move, soldiers don’t.” In the 1930s, global recession had catastrophic political consequences—in part because policymakers took exactly the wrong approach. Starting with America’s own Smoot Hawley Tariff of 1930, the world’s major trading nations tried to insulate themselves by adopting inward looking protectionist and discriminatory policies. The result was a vicious, self-defeating cycle of tit-for-tat retaliation. As states took refuge in prohibitive tariffs, import quotas, export subsidies and competitive devaluations, international commerce devolved into a desperate competition for dwindling markets. Between 1929 and 1933, the value of world trade plummeted from $50 billion to $15 billion. Global economic activity went into a death spiral, exacerbating the depth and length of the Great Depression. The economic consequences of protectionism were bad enough. The political consequences were worse. As Hull recognized, global economic fragmentation lowered standards of living, drove unemployment higher and increased poverty—accentuating social upheaval and leaving destitute populations “easy prey to dictators and desperadoes.” The rise of Nazism in Germany, fascism in Italy and militarism in Japan is impossible to divorce from the economic turmoil, which allowed demagogic leaders to mobilize support among alienated masses nursing nationalist grievances. Open economic warfare poisoned the diplomatic climate and exacerbated great power rivalries, raising, in Hull’s view, “constant temptation to use force, or threat of force, to obtain what could have been got through normal processes of trade.” Assistant Secretary William Clayton agreed: “Nations which act as enemies in the marketplace cannot long be friends at the council table.” This is what makes growing protectionism and discrimination among the world’s major trading powers today so alarming. In 2008 world trade declined for the first time since 1982. And despite their pledges, seventeen G-20 members have adopted significant trade restrictions. “Buy American” provisions in the U.S. stimulus package have been matched by similar measures elsewhere, with the EU ambassador to Washington declaring that “Nobody will take this lying down.” Brussels has resumed export subsidies to EU dairy farmers and restricted imports from the United States and China. Meanwhile, India is threatening new tariffs on steel imports and cars; Russia has enacted some thirty new tariffs and export subsidies. In a sign of the global mood, WTO antidumping cases are up 40 percent since last year. Even less blatant forms of economic nationalism, such as banks restricting lending to “safer” domestic companies, risk shutting down global capital flows and exacerbating the current crisis. If unchecked, such economic nationalism could raise diplomatic tensions among the world’s major powers. At particular risk are U.S. relations with China, Washington’s most important bilateral interlocutor in the twenty-first century. China has called the “Buy American” provisions “poison”—not exactly how the Obama administration wants to start off the relationship. U.S. Treasury Secretary Timothy Geithner’s ill-timed comments about China’s currency “manipulation” and his promise of an “aggressive” U.S. response were not especially helpful either, nor is Congress’ preoccupation with “unfair” Chinese trade and currency practices. For its part, Beijing has responded to the global slump by rolling back some of the liberalizing reforms introduced over the past thirty years. Such practices, including state subsidies, collide with the spirit and sometimes the law of open trade. The Obama administration must find common ground with Beijing on a coordinated response, or risk retaliatory protectionism that could severely damage both economies and escalate into political confrontation. A trade war is the last thing the United States needs, given that China holds $1 trillion of our debt and will be critical to solving flashpoints ranging from Iran to North Korea. In the 1930s, authoritarian great-power governments responded to the global downturn by adopting more nationalistic and aggressive policies. Today, the economic crisis may well fuel rising nationalism and regional assertiveness in emerging countries. Russia is a case in point. Although some predict that the economic crisis will temper Moscow’s international ambitions, evidence for such geopolitical modesty is slim to date. Neither the collapse of its stock market nor the decline in oil prices has kept Russia from flexing its muscles from Ukraine to Kyrgyzstan. While some expect the economic crisis to challenge Putin’s grip on power, there is no guarantee that Washington will find any successor regime less nationalistic and aggressive. Beyond generating great power antagonism, misguided protectionism could also exacerbate political upheaval in the developing world. As Director of National Intelligence Dennis Blair recently testified, the downturn has already aggravated political instability in a quarter of the world’s nations. In many emerging countries, including important players like South Africa, Ukraine and Mexico, political stability rests on a precarious balance. Protectionist policies could well push developing economies and emerging market exporters over the edge. In Pakistan, a protracted economic crisis could precipitate the collapse of the regime and fragmentation of the state. No surprise, then, that President Obama is the first U.S. president to receive a daily economic intelligence briefing, distilling the security implications of the global crisis. What guidance might Cordell Hull give to today’s policymakers? To avoid a protectionist spiral and its political spillovers, the United States must spearhead multilateral trade liberalization involving all major developed and developing countries.

#### Fragmentation of the trade order empirically causes conflict that escalate globally

Cho, Assistant Law Professor Chicago-Kent, 2007[Sungjoon, Illinois Institute of Technology "Doha's Development," 25 Berkeley J. Int'l L. 165]

Second, the mercantilist nature of the current competitive regionalism tends to evoke the strikingly similar phenomenon of the interwar period, which precipitated economic balkanization and led to the outbreak of the Second World War. n182 Highly preferential regional trading blocs instituted worldwide during this period eliminated the political space needed for multilateral economic cooperation and instead nurtured the Hobbesean struggle among major economic powers. n183 The interwar regionalist competition is a textbook [\*195] example of the prisoners' dilemma. Beggar-thy-neighbor trade policies entailed a global economic crisis that eventually exacerbated, not reduced, the evils of the Great Depression. Out of this history comes an undeniable historical lesson: the fragmented global trading system is vulnerable to a chain of unfortunate events such as tension, hostility, and violence. Considering that recent trade policies are inextricably linked to security and other foreign affairs concerns, n184 this lesson should be taken seriously lest we repeat the same historical errors and are punished for them.

#### A2: Can’t Get Material

#### It wouldn’t be difficult for Terrorists to get their hands on nuclear material.

Konkel, 2005, (Todd Konkel- professor Edmund A. Walsh School of Foreign Service, Georgetown University) “Container Security: Preventing a Nuclear Catastrophe”, International Policy Solutions, http://irps.ucsd.edu/assets/004/5372.pdf)

**A fundamental factor contributing to the threat of a container-based terrorist attack is the disturbing availability of nuclear materials, which include unsecured nuclear weapons, fissile nuclear material and other sources of radioactivity**. As previously stated, given a choice, a terrorist would opt for a nuclear device over a dirty bomb in order to maximize casualties and damage to physical infrastructure. The first obstacle a potential nuclear terrorist faces is the acquisition of a functional nuclear weapon. **There are more than two hundred locations worldwide where a would-be terrorist could acquire a nuclear weapon or the fissile material to make one**.14 The area of greatest concern is **Russia**, which **may still possess as many as twelve thousand low-yield tactical nuclear weapons that are often kept in less secure conditions** than the weapons in the nation’s strategic arsenal.15 Fortunately, a nuclear bomb in a terrorist’s hands has thus far been only the subject of spy thrillers and Hollywood productions rather than a live CNN newscast. If the theft of a complete nuclear weapon proved too difficult, terrorists could attempt to steal or purchase the necessary fissile material and construct a bomb on their own. The minimum amount of weapons-grade fissile material required for a nuclear detonation varies with bomb design but can be as little as twelve kilograms of uranium-235 or four kilograms of plutonium-239. Terrorists seeking this path might look to one of the 130 research reactors in more than 40 countries worldwide that use highly enriched uranium (HEU) as fuel.16 Attempted thefts of materials from such facilities occur with disturbing frequency. In the first three years after the fall of the Soviet Union in 1991, 6**for example, the German government reported more than seven hundred incidents of attempted nuclear sales**, including sixty cases that involved seizure of nuclear materials.17 Furthermore, the Database on Nuclear Smuggling, Theft and Orphan Radiation Sources (DSTO), compiled by researchers at Stanford University’s Center for International Security and Cooperation, has documented twenty-five “highly-credible” incidents involving the trafficking of weapons-grade plutonium or HEU since 1992.18 Fortunately, in all but one of these cases, the stolen nuclear material was recovered by law enforcement officials.

Port attack collapses the economy – political reaction ends global maritime trade

Flynn, 3. (Stephen, Commander, U.S. Coast Guard (ret.), Jeane J. Kirkpatrick Senior Fellow in National Security Studies and Director, Council on Foreign Relations Independent Task Force on Homeland Security Imperatives, 3-20-03, “The Fragile state of container security,” Testimony before the Senate, <http://www.cfr.org/defensehomeland-security/fragile-state-container-security/p5730>)

A year later I joined with former senators Warren Rudman and Gary Hart in preparing our report, “America: Still Unprepared—Still In Danger.” We observed that “nineteen men wielding box-cutters forced the United States to do to itself what no adversary could ever accomplish: a successful blockade of the U.S. economy. If a surprise terrorist attack were to happen tomorrow involving the sea, rail, or truck transportation systems that carry millions of tons of trade to the United States each day, the response would likely be the same—a self-imposed global embargo.” Based on that analysis, we identified as second of the six critical mandates that deserve the nation’s immediate attention: “Make trade security a global priority; the system for moving goods affordably and reliably around the world is ripe for exploitation and vulnerable to mass disruption by terrorists.” This is why the topic of today’s hearing is so important. The stakes are enormous. U.S. prosperity—and much of its power—relies on its ready access to global markets. Both the scale and pace at which goods move between markets has exploded in recent years thanks in no small part to the invention and proliferation of the intermodal container. These ubiquitous boxes—most come in the 40’x8’x8’ size—have transformed the transfer of cargo from a truck, train, and ship into the transportation equivalent of connecting Lego blocks. The result has been to increasingly diminish the role of distance for a supplier or a consumer as a constraint in the world marketplace. Ninety percent of the world’s freight now moves in a container. Companies like Wal-Mart and General Motors move up to 30 tons of merchandise or parts across the vast Pacific Ocean from Asia to the West Coast for about $1600. The transatlantic trip runs just over a $1000—which makes the postage stamp seem a bit overpriced. But the system that underpins the incredibly efficient, reliable, and affordable movement of global freight has one glaring shortcoming in the post-9-11 world—it was built without credible safeguards to prevent it from being exploited or targeted by terrorists and criminals. Prior to September 11, 2001, virtually anyone in the world could arrange with an international shipper or carrier to have an empty intermodal container delivered to their home or workplace. They then could load it with tons of material, declare in only the most general terms what the contents were, “seal” it with a 50-cent lead tag, and send it on its way to any city and town in the United States. The job of transportation providers was to move the box as expeditiously as possible. Exercising any care to ensure that the integrity of a container’s contents was not compromised may have been a commercial practice, but it was not a requirement. The responsibility for making sure that goods loaded in a box were legitimate and authorized was shouldered almost exclusively by the importing jurisdiction. But as the volume of containerized cargo grew exponentially, the number of agents assigned to police that cargo stayed flat or even declined among most trading nations. The rule of thumb in the inspection business is that it takes five agents three hours to conduct a thorough physical examination of a single full intermodal container. Last year nearly 20 million containers washed across America’s borders via a ship, train, and truck. Frontline agencies had only enough inspectors and equipment to examine between 1-2 percent of that cargo. Thus, for would-be terrorists, the global intermodal container system that is responsible for moving the overwhelming majority of the world’s freight satisfies the age-old criteria of opportunity and motive. “Opportunity” flows from (1) the almost complete absence of any security oversight in the loading and transporting of a box from its point of origin to its final destination, and (2) the fact that growing volume and velocity at which containers move around the planet create a daunting “needle-in-the-haystack” problem for inspectors. “Motive” is derived from the role that the container now plays in underpinning global supply chains and the likely response by the U.S. government to an attack involving a container. Based on statements by the key officials at U.S. Customs, the Transportation Security Administration, the U.S. Coast Guard, and the Department of Transportation, should a container be used as a “poor man’s missile,” the shipment of all containerized cargo into our ports and across our borders would be halted. As a consequence, a modest investment by a terrorist could yield billions of dollars in losses to the U.S. economy by shutting down—even temporarily—the system that moves “just-in-time” shipments of parts and goods. Given the c’urrent state of container security, it is hard to imagine how a post-event lock-down on container shipments could be either prevented or short-lived. One thing we should have learned from the 9-11 attacks involving passenger airliners, the follow-on anthrax attacks, and even last fall Washington sniper spree is that terrorist incidents pose a special challenge for public officials. In the case of most disasters, the reaction by the general public is almost always to assume the event is an isolated one. Even if the post-mortem provides evidence of a systemic vulnerability, it often takes a good deal of effort to mobilize a public policy response to redress it. But just the opposite happens in the event of a terrorist attack—especially one involving catastrophic consequences. When these attacks take place, the assumption by the general public is almost always to presume a general vulnerability unless there is proof to the contrary. Government officials have to confront head-on this loss of public confidence by marshalling evidence that they have a credible means to manage the risk highlighted by the terrorist incident. In the interim as recent events have shown, people will refuse to fly, open their mail, or even leave their homes. If a terrorist were to use a container as a weapon-delivery devise, the easiest choice would be high-explosives such as those used in the attack on the Murrah Federal Building in Oklahoma City. Some form of chemical weapon, perhaps even involving hazardous materials, is another likely scenario. A bio-weapon is a less attractive choice for a terrorist because of the challenge of dispersing the agent in a sufficiently concentrated form beyond the area where the explosive devise goes off. A “dirty bomb” is the more likely threat vs. a nuclear weapon, but all these scenarios are conceivable since the choice of a weapon would not be constrained by any security measures currently in place in our seaports or within the intermodal transportation industry. This is why a terrorist attack involving a cargo container could cause such profound economic disruption. An incident triggered by even a conventional weapon going off in a box could result in a substantial loss of life. In the immediate aftermath, the general public will want reassurance that one of the many other thousands of containers arriving on any given day will not pose a similar risk. The President of the United States, the Secretary of Homeland Security, and other keys officials responsible for the security of the nation would have to stand before a traumatized and likely skeptical American people and outline the measures they have in place to prevent another such attack. In the absence of a convincing security framework to manage the risk of another incident, the public would likely insist that all containerized cargo be stopped until adequate safeguards are in place. Even with the most focused effort, constructing that framework from scratch could take months—even years. Yet, within three weeks, the entire worldwide intermodal transportation industry would effectively be brought to its knees—as would much of the freight movements that make up international trade.

#### Yes Dirty Bomb

#### Strong threat of a dirty bomb

H., July 18, 2007, (H. Rosoff, works at Center for Risk and Economic Analysis of Terrorism Events, “A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach”, Wiley Online Library, <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00908.x/full>)

Since the events on September 11, 2001, the prospect of a terrorist attack using a radiological dispersal device (dirty bomb) is cited as among one the most serious terrorist threats.(1) **Several recently reported incidents confirm the concerns of security officials**. In June 2002, the **United States arrested Jose Padilla for** his **involvement with Al Qaeda in planning a dirty bomb attack on the United States**,(2) and in January 2003, **British officials found documents in the Afghan city of Herat indicating Al Qaeda successfully built a small dirty bomb as well as possessed training manuals on using the explosive device**.(3) There are several reasons why terrorists may consider **dirty bomb**s to be an attractive weapon. Radioactive **material**s are relatively **easy to obtain and** building a dirty bomb is **a** fairly **simple process**, requiring little more than the skills required for assembling a conventional bomb.(4) Furthermore, dirty bombs **can create large radioactive plumes**, cause health and psychological effects, and have major economic impacts due to the need for decontaminating large areas

#### Dirty Bomb attack results in many consequences

H., July 18, 2007, (H. Rosoff, works at Center for Risk and Economic Analysis of Terrorism Events, “A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach”, Wiley Online Library, <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00908.x/full>)

The **consequences of a dirty bomb attack** fall into three categories: (1) **immediate fatalities and injuries due to blast effects and acute radiation exposure,** (2) **medium- and long-term health effects caused by airborne dispersal of radioactive material, and** (3) **economic impacts resulting from shutting down port operations—including evacuations, business losses, property losses, and decontamination costs**. In the medium radioactivity scenario, we assumed that 5–30% of the material contained in the bomb was released into the air as aerosols or fine particulates. This results in a plume carrying roughly 500–3,000 Ci. The ranges of various damage estimates are shown in Table IV. Explanations for these ranges are provided below. We tried to be conservative on the upper end of the ranges, using information, model assumptions, and existing estimates that are at the high end. The low end of these ranges is usually self-explanatory, resulting from a failure of a successful dispersal of radioactive materials into the air.

#### Even with ways of detection, threats remain

H., July 18, 2007, (H. Rosoff, works at Center for Risk and Economic Analysis of Terrorism Events, “A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach”, Wiley Online Library, <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00908.x/full>)

**Current efforts to counter the threat of a dirty bomb attack involve plans to check all cargo for radiological materials**—both dirty bombs and actual nuclear devices.(17) For example, on June 4, 2005, Secretary Chertoff announced that the Los Angeles and Long Beach **ports will be equipped with sensitive radiological detection devices** in the form of portals to screen all international cargo entering the harbor.(18) This is certainly a step in the right direction, as radiation portals are very effective and relatively unobtrusive measures to detect even very low levels of radiation.(19) **However**, the following discussion shows that **significant threats remain**, even within the specific set of scenarios analyzed in **Port Security.**

#### Yes Smuggle

#### **Terrorist could use sea container to smuggle bomb**

Frittelli, 5-27-5 John F. Frittelli, specialist in transportation resources, science, and industry division, author; “Port and Maritime Security: Background and Issues for Congress” CRS Report for Congress, received through the CRS Web, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA453735

Much concern has focused on the threat that a sea container could be used to smuggle a nuclear weapon into the United States. Experts are concerned that if a nuclear weapon in a container aboard a ship in port is detonated, it could not only kill tens of thousands of people and cause massive destruction, but could also paralyze the movement of cargo containers globally, thereby shutting down world trade.23

#### Nuclear Terrorists are possible and could use ships to smuggle bombs

Wilson, April 08, 2010, Valerie Plame Wilson, Wilson worked for the CIA for 17 years and specialized in nuclear counter proliferation, “Nuclear terrorism is most urgent threat”, CNN,

I resigned from the CIA in 2006 because it was no longer possible to do the covert work for which I was highly trained and which I loved. This happened because in 2003, my covert identity was revealed in retaliation against my husband, Ambassador Joe Wilson, who wrote an op-ed piece in which he accused the White House of distorting the intelligence that was used to draw us into the Iraq war. But I did not lose my belief that **the danger of nuclear terrorism is the most urgent threat we face**. Nor did I lose my passion for working, albeit in a new way, to address that threat. I am working on this issue now as part of the international Global Zero movement, in which political, military and faith leaders, experts and activists strive for the worldwide elimination of all nuclear weapons. We know that **terrorist groups have been trying to buy, build or steal a bomb. In the past two decades, there have been at least 25 instances of nuclear explosive materials being lost or stolen. There is enough highly enriched uranium, or HEU, in the world today to build more than 100,000 bombs**. Terrorists looking to buy or steal HEU could look to the approximately 40 countries with nuclear weapons materials. And **then there are rogue individuals out there who are running black markets selling nuclear materials and technology. Pakistan's Dr. A. Q. Khan did it for years** before my group at the CIA brought him down in December 2003 after catching him red-handed selling a full-scale nuclear bomb to Moammar Gadhafi's regime in Libya. **If terrorists manage to get their hands on enough HEU, they could smuggle it into a target city, build a bomb and explode it. A hundred pounds of highly enriched uranium could fit in a shoebox, and 100,000 shipping containers come into the United States every day**. The nuclear threat is not limited to terrorism.

#### 1.Great threat posed by Nuclear Terrorism

Goodspeed, March 24, 2012,(Peter Goodspeed, reporter for National Post, “Peter Goodspeed: Ongoing nuclear threat looms over Seoul summit”, National Post, http://fullcomment.nationalpost.com/2012/03/24/preventing-devastating-nuclear-terrorist-attack-aim-of-world-leaders-meeting/)

 Six months after the Sept. 11, 2001 terrorists attacks on New York, Henry Kelly, then president of the Federation of American Scientists, warned U.S. leaders there may be worse to come. “Recent events make it necessary to take almost inconceivably evil acts seriously,” he told members of the U.S. Senate’s Foreign Relations Committee. In a calm, determined voice he described the **threat posed by nuclear terrorism — a risk so grave** it looms over a two-day summit of 53 world leaders that opens in Seoul, South Korea, Monday. **Terrorists or a rogue state may** some day **acquire a nuclear weapon and threaten to kill millions of people in a single devastating blow**, he said. But the **greater risk** comes **from** a malicious radiological attack or **“dirty bomb”** that uses common industrial or commercial **nuclear material to create panic, threaten the health of thousands over a prolonged period, make entire cities uninhabitable, cause billions of dollars in damage and destroy the global economy.**

#### 2.Deaths and destruction of environment

Goodspeed, March 24, 2012,(Peter Goodspeed, reporter for National Post, “Peter Goodspeed: Ongoing nuclear threat looms over Seoul summit”, National Post, http://fullcomment.nationalpost.com/2012/03/24/preventing-devastating-nuclear-terrorist-attack-aim-of-world-leaders-meeting/)

Mr. Kelly outlined what would happen **if terrorists exploded a bomb**, **containing a single, 12 inch-long, piece of radioactive cobalt** taken from a food irradiation plant, at the lower tip of Manhattan, near the former World Trade Center. “An **area of approximately one-thousand square kilometres, extending over three states, would be contaminated**,” he said. “Over an area of **about three hundred typical city blocks, there would be a one-in-ten risk of death from cancer for residents living in the contaminated area** for forty years.” “The entire borough of Manhattan would be so contaminated that anyone living there would have a one-in-a-hundred chance of dying from cancer caused by the residual radiation. **It would be decades before the city was inhabitable again**, and demolition might be necessary.” On Monday, the Seoul Nuclear Security Summit, the largest gathering of world leaders since the creation of the United Nations in 1945, aims to create a global system that will deny terrorists access to nuclear materials through improved security, decreased use of potent materials, enhanced regulatory and export controls, increased intelligence sharing, expanded use of radiation detectors and improved disposal and recycling of nuclear material.

#### 3.Nuclear Terrorism remains high

Goodspeed, March 24, 2012,(Peter Goodspeed, reporter for National Post, “Peter Goodspeed: Ongoing nuclear threat looms over Seoul summit”, National Post, http://fullcomment.nationalpost.com/2012/03/24/preventing-devastating-nuclear-terrorist-attack-aim-of-world-leaders-meeting/)

“We believe the **potential for nuclear terrorism remains high**,” said Page Stoutland, vice-president for nuclear security at the Nuclear Threat Initiative, a Washington-based think-tank. “There are **currently thousands of tons of nuclear materials in the world and those materials today are stored at hundreds of sites in over 30 countries**.” he said. “Some of those sites are well secured. **Many** are not, **leaving weapons-usable nuclear materials vulnerable to theft or sale on the black market to terrorist organizations**. “The **elements of a perfect storm are in place**: an ample supply of weapons-usable nuclear materials, an expansion of the knowledge and technical know-how to build a crude nuclear bomb accessible by the Internet or through rogue scientists and the determination of terrorists organizations to do it.”

#### 4.Theft of nuclear weapons can cause a global catastrophe

Goodspeed, March 24, 2012,(Peter Goodspeed, reporter for National Post, “Peter Goodspeed: Ongoing nuclear threat looms over Seoul summit”, National Post, http://fullcomment.nationalpost.com/2012/03/24/preventing-devastating-nuclear-terrorist-attack-aim-of-world-leaders-meeting/)

“With highly enriched uranium, a gun-type bomb — like the one that obliterated Hiroshima — is very plausibly within the capabilities of a sophisticated terrorist group,” he said. With weapons-usable **nuclear material** stored in hundreds of buildings in dozens of countries, **under security situations that range from very stringent to virtually non-existent, the risk of terrorists acquiring bomb-making materials remains great.** “**Theft of only 0.01% of the world stockpile could cause a global catastrophe**,” Mr. Bunn said. And **terrorists have shown a definite interest in obtaining the materials** needed to make both nuclear fusion and radioactive dirty bombs.

#### 5.Radioactive materials going missing now

Goodspeed, March 24, 2012,(Peter Goodspeed, reporter for National Post, “Peter Goodspeed: Ongoing nuclear threat looms over Seoul summit”, National Post, http://fullcomment.nationalpost.com/2012/03/24/preventing-devastating-nuclear-terrorist-attack-aim-of-world-leaders-meeting/)

“**In the United States, a radioactive source is lost, stolen or missing about once a day**,” said Charles Ferguson, current president of the Federation of American Scientists. **Khammar Mrabit, head of the International Atomic Energy Agency’s Office of Nuclear Security, said he investigates roughly 200 incidents of improperly secured nuclear material each year**. “The **threat of malicious radiological attack is quite real, quite serious and deserves a vigorous response**,” Mr. Kelly warned 10 years ago in the aftermath of Sept. 11. “We must face the brutal reality that no technological remedies can provide complete confidence that we are safe,” he said. “Determined malicious groups might still find a way to use radiological weapons when their only goal is killing innocent people.”

#### Container Security Impacts

#### Unsecure containers increase the risk of clandestine proliferation

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)

Despite terrorism recently becoming a primary port concern, containers are notoriously and continuously used for other criminal purposes. Shipping containers are used to ship illegal drugs, arms and munitions, undocumented workers, and even nuclear equipment and technology. 53 One of the most unsettling, suspected uses of shipping containers was by former-Pakistan nuclear program head, Abdul Qadeer Khan. 54 Khan, who admitted to selling nuclear technology to Iran, Libya and North Korea 55 is suspected of having used shipping containers to complete these sales, including a shipment inspected in August 2003 in the Mediterranean. 56 The shipment allegedly included the transport of elements of a future Libyan nuclear plant. 57

#### Terrorist attacks on Ports devastate regional economies

Council on Foreign Relations, Jan. 2006 (“Targets for Terrorism: Ports” Backgrounder http://www.cfr.org/port-security/targets-terrorism-ports/p10215)

Yes. Experts warn that U.S. seaports could be tempting targets for terrorists bent on killing large numbers of people, grabbing media attention, and disrupting the U.S. economy. Port, ferry, and cruise-ship terminals are often located in highly congested areas where large numbers of people live and work. Liquefied natural gas terminals and refineries that produce highly volatile petrochemicals and convert crude oil into gasoline and heating oil are also often nearby. Given the importance of foreign trade to the U.S. economy, an attack that shut down a major American port for even a few days could devastate the regional economy served by that port.

### Solvency – PSGP

#### Solves Generally

#### Current security is uncoordinated – PSPG grants necessary to assist ports in infrastructure improvements

Logistics Management 7/10/2010 (“U.S. Port Security: A work in progress” Logistics Management ProQuest)

Port authorities contend that without a method of enforcement, supply chain security has little chance of truly enhancing safety. Here's a closer look at the different paths U.S. ports are taking in route to establishing standards and adhering to new regulation mandates. Americas seaports arc taking several different paths toward providing shippers with safe and secure commerce. And while some are more heavily reliant on sophisticated container screening systems, others are concentrating on vetting sup?Iy chain partners and intermediaries. At the same time, all ports are mandated to comply with new U.S. regulatory rules while remaining poised to anticipate new changes in international law. Any way you slice it, security will continue to be a market differentiator and competitive tool for our ocean cargo gateways well into the future. However, since there are an estimated 360 seaports in the U.S., no single security solution fits every gateway, says American Association of Port Authorities (AAPA) spokesman Aaron Ellis. "Some ports are dealing solely with bulk and break bulk cargo, so container scanning is not going to work," he says. "And others may chiefly have roll-on/roll off and project cargo," he adds. "But for the major container ports, the standards are fairly uniform." Joe Lawless, the Massachusetts Port Authoritys (Massport) director of maritime security, agrees with Ellis, adding that 100 percent container screening will have to be customized to be effective. "Some ports will concentrate on screening for radiation, while others will place a higher emphasis concentration on routine inspection," he says. "In any case, its one of the critical pieces that's only being worked out right now." Lawless, who also serves as chairman of the AAPAs Port Security Committee, will be meeting with his colleagues in New Orleans this month to discuss other is- sues related to port protection. Seaports worldwide annually handle roughly 1.5 billion tons of cargo worth more than $1 trillion, arriving in at least 11 million containers. They require deep-water access, sufficient land for staging and storage, and unrestricted access to highway, rail, inland waterway, and pipeline networks. At this point in time, the Department of Defense (DoD) maintains only an informal business relationship with U.S. ports. However, the DoD plays a considerable role in the security plan to prevent attacks on the ports, prepare to respond to possible attacks, and to restore their services post attack. "But the ports themselves have to help government determine what the priorities arc," says Lawless. "Thats why AAPA members must constantly network among ourselves and our overseas counterparts to share information." More fed support The AAPA endorses the current federal strategies and supports even stronger protection measures, but not without some caveats and suggestions. "The Port Security Grant program (PSGP) continues to be very valuable and serves as a partner with the Department of Homeland Security (DHS) to harden security at U.S. ports and to protect our homeland," says AAPA president and CEO Curt Nagle. "But the cost must be shared." The PSGP funds are primarily intended to assist ports in enhancing maritime domain awareness, enhancing risk management capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices as well as training and Transportation Worker Identification Credential (TWIC) implementation. According to the AAPA, this can best be achieved with what it calls "Cost-share Waiver," as ports do not have the money to contribute more than they are spending right now. Presently, says the AAPA, a 25 percent cost-share for public agencies is "a significant economic disincentive" to make security enhancements and implement regional maritime security plans. In these tight economic times, the cost-share is an even greater problem as ports are cutting back in all areas to address economic shortfalls, authorities note. The Port Security Grant program is one of the few DHS grant programs that requires a cost-share. Transit grants and state homeland security grants, for example, are exempt from cost-share requirements. At the same time, say port authorities, funding is key. They advocate a plan that will continue to appropriate $400 million for the program as authorized in the SAFE Port Act. "All ports should be eligible for these funds to avoid a soft underbelly that leaves this country vulnerable to terrorist threats," says Nagle. "Grant funding should be better tied to port area strategic plans and funding should be made available for resiliency and business continuity projects." Part of this, of course, involves a quicker distribution of funds, too. Currently, there is a significant time delay between when DHS announces the awards and when FEMA finally completes all reviews and gives grantees authority to begin these security improvements. According to the ports, DHS should work to streamline their processes and get funding out more quickly. Command centers Broader construction costs to improve security should be allowed if progress is to be made swiftly, according to the AAPA. "The current limits on construction projects-$1 million or 10 percent of the total grant-should be eliminated. This is especially important for the stimulus funding, since Congress placed a priority on construction," argues Nagle. He further maintains that personnel costs should be an allowable expense, adding that DHS allow grant funds to be used for personnel costs, as provided in the Maritime Transportation Security Act and SAFE Port authorization legislation. This way, he says, DHS can mirror both the Urban Area Security Initiative and Transit Security Grant Programs. In a recent statement, the AAPA urged legislators to consider allowing ports to hire new security personnel (staff for operations, fusion or emergency centers, planners, counterterrorism posts, etc.) for the term of the grant. Personnel costs, authorities further state, should also be permitted to backfill salaries for approved training programs. Part of this manpower initiative also involves the U.S. Coast Guard. The SAFE Port Act calls for the U.S. Coast Guard to establish command centers. At the same time, some ports are developing their own centers. AAPA members argue that better coordination is needed between the Coast Guard and the Area Maritime Security Committees on the Coast Guard plans, as well as with those who arc building command centers based on Port Security Grant funds. "The U.S. Coast Guard must take a stronger role in controlling risk from small vessels that transit commercial port areas," says Nagle. "While the Coast Guard has had several public meetings, more needs to be done to control this risk." Supply chain security reality check Is it now time for a supply chain security reality check? AAPA certainly thinks so. "While the DHS has attempted to address supply chain security under the various programs that have been promulgated by Customs and Border Protection (CBP), the reality is that no internationally agreed-upon minimum supply chain security standards have been established" says Nagle. He contends that without this global baseline and a method of either enforcement or rewards, supply chain security is largely a voluntary notion that has little chance of truly enhancing safety. Nagle and his constituents suggest that a framework for minimum mandatory supply chain security standards that is recognized and accepted worldwide is necessary in order to begin the complex process of ensuring that goods moving through the supply chain are not compromised. According to Nagle, this framework would cover five major areas: 1. Verification that a container is free of false compartments. 2. Verification that reasonable care and due diligence has been used in packing, securing, and manifesting goods. 3. Ensuring that the cargo has not been tampered with at any point along the route. 4. Ensuring that the integrity of the information and information systems associated with movement of cargo has not been compromised. 5. Ensuring that accurate data on the shipment is provided to Customs well in advance of the ships arrival in the U.S. In terms of policy, Nagle is hardly alone. Donald Masters, Ph.D., a board member of the Homeland Security Innovation Association (HLSIA), says that the U.S. should more proactively engage multilateral organizations to adopt reasonable and attainable international standards for detection equipment performance as well as procedures for their effective use. "The U.S.-EU Agreement calls for greater regional cooperation," he says. "This needs to move forward with an operational protocol that specifies port requirements that meet the mutually agreed upon standards for secure transatlantic trade." According to Masters, a regional consensus on equipment standards and port procedures could then be expanded through the World Customs Organization. That, in turn, would make operational the already existing agreement known as the "Framework of Standards to Secure and Facilitate Global Trade." "Alternatively, the U.S. could make use of other regional agreements, possibly under ASEAN or APEC auspices, with major Asian trading partners," says Masters. "Such negotiations will require patience and perseverance but if successful, they will make trading partner countries fully responsible for the safety and security of their exports." An offshore port security system, adds Masters, would he far more cost-effective for the U.S. than the current patchwork of bilateral agreements involving the deployment of CBP teams and costly U.S. supplied equipment. The nuclear threat As far as scanning equipment goes, ports are uniformly saying that CBP and the Department of Energy should work more closely with port facilities as they develop next generation detection systems. This, the ports add, would ensure that they work well with port operations. AAPA encourages DHS to carefully evaluate the viability of the 100 percent scanning mandate and avoid instituting a system that will slow cargo movements or significantly increase the cost of shipping. AAPA, of course, is also concerned about reciprocity. Will China, for example, require stricter standards on U.S. exports if we go too far in complicating the supply chain? The DHS Domestic Nuclear Detection Office has been working with ports on nuclear detection, but U.S. port authorities say more should be done to identify ways to mitigate the risk of nuclear weapons when such weapons are suspected in a shipment. As a best case scenario, DHS could work with ports on the protocols that they use and encase and shield a suspect container that is being shipped to an inspection area. At the same time, AAPA continues to work with DHS on implementing the TWIC program, including monitoring and commenting on Coast Guards regulations for facility compliance with TWIC. As the federal government seeks to apply its resources to port security issues, multiple programs and multiple agencies have become involved through homeland security programs. In order to ensure that these are adequately managing the risk associated with port security, a security system model is needed to guide its partners/stakeholders, both government and private, in the effective and efficient development and implementation of holistic port security solutions. According to port authorities and their private sector partners, this security system model should include a coordinated approach, employee business models, and be bi-directional. Federal plans should also encourage strategic plans for port security. "Partnering with the port industry in the development of systems-based integrated solutions, the federal government can avoid vendor-driven programs by communicating with port stakeholders from concept to execution to ensure that the dynamic needs of ports are met through a team approach," adds Nagle.

#### Funding is being allocated inefficiently—while ports are vital to national security, their funding is either unspent, cut, or forgotten

Wallman 11[Brittany, “Wasserman Schultz Blasts Port Security Budget Cuts,” Web, 3/8/11, South Florida Sentinel, Proquest, 6/20/12]

"1.4 billion dollars remains ready for us, **unspent, in protecting America's ports,**" a statement from his Washington, D.C., office says. "**This means the Obama Administration has failed to allocate $1.4 billion into port security. That, along with the fact that Congressional Democrats failed to pass a budget last year, should be our focus, and should be of major concern** for the American people." Democratic Congresswoman Debbie Wasserman Schultz blasted Republicans' proposed 2011 budget Monday, saying one of the many cuts would crimp security at Port Everglades and in ports across the country. Wasserman Schultz, D-Weston, said **a two-thirds slicing of the national Port Security Grant Program would translate to a loss of $1.5 million** for Port Everglades. **Those grants are not used for day-to-day security, but pay for new projects and technology.** Standing in the port in front of a foreign cargo ship, with heavy trucks roaring by, she said "**a tight web of security" at the nation's ports is essential to the safety of the community, and also to the economy**. Since the Sept. 11, 2001, terrorist attacks, Port Everglades security has been beefed up substantially. "**Why would we go backwards?**" she asked. Broward Sheriff Al Lamberti, a Republican, joined her, saying the port is Broward County's economic engine, and that "**if the port fails, the country fails."**

#### Inefficient and slow grants and cost-share programs make current security ineffective

PR Newswire 2011 (American Association of Port Authorities, “10 Years After 9/11, Security Still a Top Priority of U.S. Ports” Lexis 6/19/12)

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. "For centuries, seaports have been a vital part of this nation's transportation infrastructure, and safe, secure seaport facilities are critical to protecting our borders and moving goods," said Kurt Nagle, American Association of Port Authorities' president and CEO. "Regrettably, the more than 50 percent funding level cut recommended for FEMA's State and Local Program grants, which includes the Port Security Grant Program, could impact the current security capabilities of many U.S. ports as well as hamper their ability to carry out their five-year port protection plans." 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." Security Improvements Significant, But Costs High The comprehensive Maritime Transportation Security Act 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. While federal Port Security Grant Program funds have helped pay for the sweeping security overhaul at U.S. ports, the grants oftentimes require ports to pay a 25 percent "cost-share," pay 100 percent of their security program operations, management and policing personnel expenses (representing the highest ongoing cost for security at most ports), and limit infrastructure construction costs to 10 percent of the grant total. Furthermore, in addition to the huge funding cuts proposed for fiscal 2012 and beyond, the lumping of port grant funds with other State and Local Program grants-such those for first responders, urban areas and transit systems-will likely result in even less funding for port security. Although insufficient security grant funding is a chief concern among ports, there is also a significant concern about the time delay between when DHS announces grant awards and when it completes all reviews and gives grantees authority to begin their security improvements. Consequently, AAPA has urged DHS to streamline their processes and get funding out more quickly.

#### Reform Solves

#### ( ) Program strat inefficient only the plan solves

Office of the Inspector General, January 2010 (Office of the Inspector General, “Review of the Port Security Grant Program,” Department of Homeland Security, http://www.oig.dhs.gov/assets/Mgmt/OIG\_05-10\_Jan05.pdf)

The Port Security Grant Program provided funds for security within the maritime industry, generated additional investments, and significantly increased awareness of security needs. With no shortage of potential projects to choose from and limited funding, the program strove to award funds to projects that best matched its eligibility criteria. We observed good, respectful, working relationships among TSA, USCG, and MARAD, who collaborated to stand up a competitive grant program and leverage their expertise throughout multiple rounds of grant awards. However, the program’s strategic impact is less apparent and its purpose and goals require refinement to support national priorities effectively. Specifically: 1 This includes $75 million made available by the Department of Homeland Security’s Office for Domestic Preparedness. Review of the Port Security Grant Program Page 3 2 P.L. 107-295. Page 4 Review of the Port Security Grant Program • While the program’s eligibility criteria are directed broadly at national critical seaports, the current design of the program compromises the program’s ability to direct resources toward the nation’s highest priorities. • The program is attempting to reconcile the goals of the Maritime Transportation Security Act of 2002 (MTSA), 2 the competitive grant program mandated by Congress, and risk based direction of grant monies. MTSA is a nationwide security mandate that widely affects the maritime industry. The program is faced with the competing pressures of offsetting MTSA related costs while making competitive and risk based grant decisions to protect the nation’s most critical ports and port facilities.

• The program did not have the benefit of national key asset and critical infrastructure protection information now being developed by the Information Analysis and Infrastructure Protection (IAIP) directorate. Program administrators and IAIP, which is responsible for developing strategies for protecting the nation’s critical infrastructure, did not collaborate to integrate the program with broader national security initiatives. • Grant award decisions are made with the intent of expending all available funding and spreading funds to as many applicants as possible. The program funded projects despite dubious scores by its evaluators against key criteria, raising questions about the merits of several hundred projects. Frequently, headquarters and field reviewers did not agree about the eligibility or merit of projects and did not consistently document their rationale for recommending or not recommending funding. • The question of where the private sector’s responsibility for preventing terrorism ends and where the federal government’s responsibility begins poses a dilemma for the Port Security Grant Program. DHS does not have a formal policy to provide financial assistance to private entities, a group that includes those that own and operate high risk facilities. Private entities have applied for and received substantial funding. Some of that funding went to projects that reviewers scored below average or worse during the evaluation process. • At each level of the application review process, reviewers were challenged to meet short deadlines to evaluate, rate, and rank projects. This affected the ability of reviewers to document thoroughly their decisions and made subsequent levels of review more difficult. • After three rounds of the Port Security Grant Program, recipients spent only a small portion of the entire amount awarded. Of the $515 million awarded between June 2002 and December 2003, including $75 million provided under the Office for Domestic Preparedness’s (ODP’s) Urban Area Security Initiative (UASI), grant recipients had expended only $106.9 million, or 21% of total program awards as of September 30, 2004. As a result, the majority of projects have not been completed and the program has not yet achieved its intended results in the form of actual improvements to port security. • Following TSA’s second round of grant awards in 2003, ODP made $75 million available for port security grants under the UASI. The UASI is distinct from TSA’s program and had not been used for port security grants previously. ODP, in consultation with TSA and the Office of State and Local Government Coordination, 3 utilized a risk based approach, 4 which differed from the program’s original competitive process, to select 14 eligible port areas and the corresponding funding amounts for each area. TSA then provided unfunded applications from its second round of grants to ODP, which in turn, funded 86 projects. The TSA, USCG, and MARAD National Review Board had reviewed these projects before they were submitted to ODP and determined that 82 did not merit funding. • Secretary Ridge moved TSA’s Port Security Grant Program into the Office of State and Local Government Coordination and Preparedness (SLGCP). SLGCP officials would like to combine elements of ODP’s discretionary risk based approach with TSA’s competitive program that relies on USCG and MARAD expertise for making grant award decisions. It is not clear how SLGCP will combine the elements of these programs. 3 The Office of State and Local Government Coordination and the ODP were moved into the Office of State and Local Government Coordination and Preparedness on May 17, 2004. 4 The UASI Port Security Grant Program is distinct from the primary UASI grant program. The primary UASI grant program identified and awarded formula grants to 50 high threat urban areas. The program utilized a different methodology to derive the funding amounts for the 14 selected port areas. Review of the Port Security Grant Program Page 5 Page 6 Review of the Port Security Grant Program • Port security grants were awarded through two different statutory authorities, TSA’s appropriation and ODP’s UASI program, which have different award processes and eligibility requirements. A third authority, MTSA, mandates security requirements for port facilities and vessels and contains another grant authority intended to offset the costs of the security mandates. The consolidation of ODP’s UASI program and TSA’s Port Security Grant Program into SLGCP and the impact of MTSA cloud the statutory intent and future direction of port security grants. We are recommending that the Executive Director, Office of State and Local Government Coordination and Preparedness: Recommendation #1: Determine to what extent the program should incorporate MTSA requirements. Recommendation #2: Incorporate critical infrastructure and key asset data from IAIP into the evaluation of proposed port security projects. Among the changes to consider: • • • The addition of an IAIP official on the Executive Review Board; Use of the IAIP national asset database to identify critical facilities in need of mitigation with a view toward soliciting proposals from these facilities; and Collaborating with IAIP in an outreach program to improve the quality of vulnerability assessments and proposals. Recommendation #3: Consider changing the weighting of the evaluation criteria, with greater emphasis placed on the criteria that reduce critical vulnerabilities. Recommendation #4: Cease the practice of funding projects that do not meet the definition of a Priority I project. Consider implementing a scoring threshold that ensures that projects not meeting that threshold are not funded. Consider seeking a change in appropriations language to have these grant funds designated as “no- year monies” to reduce the impetus to fund doubtful projects. Recommendation #5: Require reviewers to document their decisions in the grants management system, particularly when they are inconsistent with recommendations from a lower level of review. Recommendation #6: Develop parameters that define applicant eligibility under the “nationally important economic port or terminal,” “responsible for movement Background 5 P.L. 107-71. 6 P.L. 107-117. of a high number of passengers,” and “responsible for the movement of hazardous cargo” criteria. Recommendation #7: Communicate information to field reviewers to educate them on eligibility. Improve dissemination of “lessons learned” at all levels of review. Recommendation #8: Evaluate timeframes for reviewing applications with an emphasis on providing more time for review in the field and by the ERB. Recommendation #9: Clarify department policy on funding private sector projects. In the absence of such policy, and if funding private sector projects is continued: (1) examine private sector projects to preclude the funding of cost of business expenses; (2) develop financial eligibility criteria, including an income test or cost-benefit analysis; and (3) consider giving greater preference to projects that are submitted jointly by private and public entities. Recommendation #10: Accelerate the acquisition of more information from applicants about the scope of their projects. Recommendation #11: Ensure that the program has sufficient operational expertise to administer the program after the award is made. Recommendation #12: Seek clarification on the legislative intent for the program (sector-specific vs. larger infrastructure protection initiatives) and construct a unified program (policy, purpose, process, and eligibility) to comply with that intent.

#### Problems with distribution of funds make the program inefficient reform solves

Richardson 12-29-11 (Whit Richardson, managing editor of Security Director News, freelance journalist covering various topics, business writer at a statewide magazine, “Report Cites Flaws in DHS Port Security Grant Program”, Security Director News, http://www.securitydirectornews.com/public-sector/report-cites-flaws-dhs-port-security-grant-program)

The report also notes FEMA's problems distributing the funds. Of the roughly $1.7 billion awarded by FEMA between 2006 and 2010, only 23.6 percent has been drawn down by grantees, while 24.3 percent (or about $400 million) remains "unavailable" to grantees, according to the report. The remaining 52.1 percent is funding that has been allocated, but has yet to be drawn down by the grantees. Of the $400 million that is "unavailable,” the funds are either "unused" or "on hold." Unused funds have yet to be allocated to specific projects, while on-hold funds are unavailable because grantees have yet to meet post-award requirements, such as environmental reviews. One thing to remember is that the PSGP is a draw-down program, meaning ports have to put up the money first before they can actually go out and get paid back for their expenses, Aaron Ellis, spokesman for the American Association of Port Authorities, told SDN. "A lot of times the permitting process can take a couple years," he said. One of the issues contributing to the amount of unused funds, according to the report, has been the inconsistent cost-share requirement of grantees. While cost-share requirements were waved for fiscal years 2010 and 2011, previous years required a match. In the economic downturn, many grantees chose not to pursue the funds, especially once they knew that future monies would not carry the requirement, according to the report. The AAPA has consistently lobbied for the elimination of the cost-share requirements, which Ellis points out do not exist for the transit security and state homeland security grant programs. "Particularly in these tight economic times, the cost share is a challenge for ports that are cutting back in all areas to address economic shortfalls," Ellis said.

#### Grants needed to be streamlined and increased

Holmes 12 (Captain John Holmes, Deputy Executive Director of Operations for the Port of Los Angeles, AAPA, <http://appropriations.house.gov/uploadedfiles/hhrg-112-ap15-jholmes-20120307.pdf>)

FEMA and ports are working hard to resolve this draw-down problem. Two key things that could speed spending are providing a uniform cost-share waiver and further streamlining the FEMA Environmental and Historic Preservation (EHP) review process. As you know, some years there is a cost-share requirement, and other years it is waived and grantees must go to DHS for a project-based waiver. This significantly delays the use of funds and some grantees wait to see if they can get cost-share-waived funds before undertaking a project. AAPA strongly endorses a uniform waiver of cost-share for all past grants to stimulate quicker use of past funds. Another hurdle is the EHP review within FEMA. While other FEMA programs must go through these reviews, there isn’t the threat of a loss of funds, because there is no timetable associated with these other programs. Therefore, the EHP reviews are not processed or prioritized in a way to reflect grant time limitations. Additionally, FEMA EHP reviews could be streamlined by taking into account state and local environmental reviews for a facility. While EHP has streamlined some of their reviews, they still are a major reason why many of the grant projects require an extension. Port Security Grants are managed quite differently than other homeland security grants. Priorities are set locally, based on the risks and vulnerability of the local port area. Other homeland security grants have a list of core capabilities, which all grantees try to attain. This capabilities list is based more on movable and shared assets rather than set facilities. There is no such list of core capabilities for port security grants and the ones developed for other grant programs were not developed with ports in mind. Additionally, ports have certain federal mandates, such as TWIC readers, that they must comply with, and the cost of those requirements will not be fully felt until Coast Guard issues its final regulations. Not only does a second or potentially third pass-through layer (the State or municipal government, respectively) mandate its own sets of compliance requirements on top of Code of Federal Regulations and Office of Management and Budget Circulars, it also creates unnecessary cogs in the administration that slows down our ability to spend, execute, and deliver. Moving funds to the states would compromise program efficiency and effectiveness. If, however, a decision is made to consolidate the program and move it to the states, AAPA strongly urges your Committee to allocate a set amount of funding for the program to ensure that funding for port security is not diluted further. We appreciate the willingness of DHS to work with the ports on Port Security Grant issues. We have and will continue to work with them to improve the program. Positive changes have been made, and we hope that these changes will continue. We do feel that over time external pressures and the “pile-on” effect of new and continuing requirements has had a significant negative impact on the program. We also believe that it is an appropriate time for a DHS/Grant User Group to conduct a review of the Port Security Grant Program and identify areas of improvement and recommend changes that will address these areas.6 For Fiscal Year 2013 and beyond, we strongly urge the Committee to: 1. Restore port security funding to its earlier level; 2. Keep the funding separate, similar to Firefighter Assistance Grants; 3. Maintain current federal control over program, or if funds are moved to the States, appropriate a set amount for our nation’s ports; 4. Consider a uniform cost-share waiver of past grant funds; and 5. Establish a joint DHS/Port group to continually streamline the process. In order to continue to be effective, the grant process must evolve in conjunction with port needs and vulnerabilities. Working with DHS, efforts have been made to keep pace with this evolution. We fear that if ports are “lumped” into the larger Homeland Security equation, efforts to date will be marginalized and the focus on ports will be lost. The separation of Port Security Grant funding served to highlight the need to focus on a component of the nation’s critical infrastructure that was largely ignored prior to the tragic events on 9/11. We have a significant fear that this focus will be lost if the Port Security Grant Program does not remain separate and fails to continue to evolve to meet emerging security needs.

#### Funding Solves

#### Increasing funding the PSGP solves

NASBLA, March 2011 (National Association of State Boating Law Administrators, “Port Security Grant White Paper March 2011” NASBLA, http://nasbla.org/files/public/Prepardness%26Repsonse/White%20paper%203-14-11.pdf)

Earlier this month, the House of Representatives passed HR 1, the continuing resolution for the FY11 budget. Among many other cuts, the legislation reduces funding for the Port Security Grant program by two-thirds; bringing the funding level down from $300 million to $100 million. Just a few days ago, the Senate rejected this proposal, but also failed to pass an alternate version. If the House and Senate do not reach a compromise by March 18, 2011, the Federal government faces a shutdown. The purpose of the Port Security Grant Program is to create a sustainable, risk-based effort to protect critical port infrastructure from terrorism. The program provides grant funding to port areas for the protection of critical port infrastructure from terrorism and are primarily intended to assist ports in enhancing maritime domain awareness, enhancing risk management capabilities to prevent, detect, respond to and recover from attacks. Action In this brief window of opportunity, NASBLA and its members must urge policy makers to make the right choice and keep Port Security Grant Program funding levels on par with previous budget proposals. In addition to the necessity of the Port Security Grant Program for ensuring the security of our nation’s ports and waterways, the grant dollars made available also enable the Coast Guard to actively partner with state and local law enforcement. Last year Congress passed the 2010 Coast Guard Authorization Bill, which included language directing the Commandant to establish national standards for training and credentialing law enforcement personnel to enforce a security zone or assist in such enforcement. It also requires the Commandant to develop training curriculum to test and deliver such training. Currently, the only Federal resources available to achieve these mandates are monies derived from the Port Security Grant Program. Not only are the Federal dollars needed to maintain current initiatives, but they are vital in further developing initiatives with state and local law enforcement to better secure our nation’s borders. It is imperative that Congress not cut any monies from this program and instead maintain the same level of rigorous commitment to securing our nation’s waterways as previous Congresses have shown.

#### Grants Increase Security

#### Grants increase US security

Mayer 2-14-12 (Matt Mayer; researches, writes and speaks on national security issues as a visiting fellow at Heritage, president of Provisum Strategies, writer, senior official at the Department of Homeland Security; “Proposed Revisions to Homeland Security Grants Make Sense”; The Heritage Foundation; http://www.heritage.org/research/ reports/2012/02/reforming-thehomelandsecurity-grants-program)

The Obama Administration’s adoption of much of the previous Administration’s policies on fighting the war against terrorists is well known. Less well known is the increasing move toward other homeland security grant policies formulated in 2005 and early 2006. These moves, including the adoption of a risk and need model for allocating homeland security grants, are to be rightly applauded, as these reforms ultimately increase the security of America. The new direction includes an important focus on “critical infrastructure and key resource protection and long-term vulnerability reduction” and prioritizing support to local counterterrorism activities.

#### Federal Gov’t Key

#### **Only USFG can effectively work on port security**

Holmes 12 (Captain John Holmes, Deputy Executive Director of Operations for the Port of Los Angeles, AAPA, <http://appropriations.house.gov/uploadedfiles/hhrg-112-ap15-jholmes-20120307.pdf>)

Moving the funding to the states is also a big concern for AAPA. Port security is focused

on protecting international borders. This is a federal responsibility, not a state

responsibility. Many States don’t have the personnel or expertise to evaluate maritime

risks or determine how ports should be prioritized against other homeland security

priorities in the state. The risk evaluations for ports are made at the federal level by the

U.S. Coast Guard and other federal agencies. We are also concerned that this would

increase the complexity in grant management and slow a process that is already

recognized as cumbersome.

### Solvency – Voluntary Incentives

#### 1ac Stuff

#### The United States Federal Government should increase its investment in transportation infrastructure by giving financial incentives to shipping companies to improve port functioning.

#### Contention 2 is Solvency

#### Broad mandates instead of specific guidelines are key – it allows technology to progress over time.

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

A large number of companies are vying to provide trade-security solutions. They offer a bewildering array of products, from tamper-evident chemical seals to strong mechanical locking mechanisms to advanced satellite-tracking technologies. The most interest and attention, however, has revolved around efforts to create a “smart container” that greatly improves the ability of shippers, cargo owners, and Customs agents to know when a container has been opened or diverted. Smart containers offer the promise of strong security from the time a container is loaded until the time it reaches its final destination. The most basic smart containers would probably incorporate passive radio frequency identification (RFID) tags—technology similar to that used to track cars through toll lanes—that would be read by either handheld or stationary scanners. The RFID tags would store information about the container’s contents and its travels. More advanced RFID solutions would include a hybrid electronic/mechanical seal that both bars and detects unauthorized container entry. If a container is opened during transit, the seal would record information about when (and possibly where) the intrusion occurred. Passive RFID technology has several advantages, including relatively low cost and proven operational capability. Tags are activated by scanners and thus do not require a power source. Passive seals have drawbacks, too. They provide for only limited tracking of containers in transit. Stakeholders can see when a particular container arrives at a port, warehouse, or other scanning station, but real-time tracking is not available with passive RFID and containers do not alert anyone at the moment they are compromised. More sophisticated smart containers could include active electronic seals. These devices would detect when someone breaks into a container and would have the ability to communicate that information to a shipper, customs, or cargo owner via satellite, radio, or cellular—or conceivably, even local Wi-Fi computer networks installed on ships and at ports. In the most advanced versions, cargo containers could be outfitted with Global Positioning System devices for precise location tracking and sensors to detect and alert authorities immediately to the presence of chemical, biological, or nuclear elements. A Wall Street Journal article recently described how active-seal smart containers might work: [A smart container] could say, ‘Hey, someone has taken me to a place off my route, and I was there for two days. Is that OK?’ says Blair LaCorte, an executive vice president of Savi Technology Inc. The Sunnyvale, Calif., company has already set up a system using radio-frequency identification technology to track about 25,000 containers a day for the Department of Defense. Such systems include a radio transmitter and receiver on the container, which is linked to a central data system.75 Not surprisingly, active-seal technology is more expensive than passive-seal technology— up to 10 times more expensive, according to the U.S. Treasury’s Advisory Committee on Commercial Operations of the U.S. Customs Service.76 Active seals also require a power source and are unproven on a mass scale. Fortunately, DHS need not mandate a single solution. As long as a seal can communicate with CBP scanners, it does not necessarily matter whether a container uses active or passive technology. Nor is it critical that all containers have exactly the same package of features. By setting standards and avoiding overly detailed mandates, DHS can preserve a dynamic, competitive marketplace for smart-container technology that continues to yield advances over time.

#### 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.

#### Creating incentives is key to increase port security

Flynn, 4/2/2008 (Stephen, Jeane J. Kirkpatrick senior fellow for National Security Studies at the Council on Foreign Relations “Overcoming the Flaws in the U.S. Government Efforts to Improve Container, Cargo, and Supply Chain Security” Written Testimony before a hearing of the Homeland Security Appropriations Subcommittee, Committee on Appropriations, United States House of Representatives)

In charting a way forward, it is essential to be mindful of the extent to which private companies and our trade partners have an enormous stake in how we approach the challenge of container, cargo, and supply chain security. The conventional wisdom that security within the global transportation and logistics system is more of a public sector responsibility than a private sector one is wrong. This conventional wisdom persists in no small part because Congress and U.S. enforcement agencies want to be in the driver’s seat in managing the security imperative. In practice this translates into “public-private” partnerships involving the public sector setting the requirements and the private-sector being asked to cheerfully embrace the costs of complying with them. This process needs to be reversed. For the intermodal transportation industry and companies with supply chains that rely on the industry, cargo and container security has become an important business continuity risk. They must be provided with the incentives for taking the lead in developing solutions that manage that risk while government plays a support role. An example of this is a recent effort by the Port of Los Angeles to reach out to Hutchison Port Holdings, the largest terminal operator in the world, to develop a joint port industry effort to improve container security. Specifically, the Port of Los Angeles is interested in finding a way that terminal operators might invest in and maintain active and passive scanning equipment to examine the contents of containers as they enter their yard. The idea is that if these images could be routinely collected by the terminal operator, when government authorities want to examine the contents of a container, these officials could “pull the bits, instead of pulling the box.” That is, inspectors could look at the images of the targeted containers collected by the terminal operators. In the vast majority of the cases the images would reveal there is no dense material and therefore there is no risk that the container is carrying a nuclear weapon or shielded material. These containers could then be immediately cleared for loading without their having to be removed from the stacks. Everyone wins. The terminal operator benefits by minimizing the risk of its yard will be disrupted by these inspections. The ocean carrier benefits by having no disruption to its loading plan. The importer benefits by not having the risk that its container will miss the voyage. Finally, CBP benefits by being able to conduct more inspections under the CSI protocol than the current circumstances allow.

#### A2: Delay

#### Delays are not a concern with top importers

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)

With the CSI in place, much of the concern from importers relates to potential delays to the supply chain due to the use of detection technology at the ports of entry. Bennett and Chin (2008) state that there are also concerns about innocent alarms. Gerald Epstein, a homeland security expert for the Center for Strategic and International Studies, commented, “There are an awful lot of things that are radioactive out there… if all you’re doing is looking at the total amount of radiation, you are going to be opening up a lot of boxes and finding kitty litter” (p.31). In interviews conducted by Bennett and Chin (2008) with several of the top 10 importers in the United States to get a better understanding of their opinions on current security programs, the majority of the importers state that delays are not currently an issue in the maritime transportation mode even with these additional new initiatives. Sporadic delays have occurred due to increased scanning and inspection, but are not yet of great concern (p.43).

#### Tech Solves

#### Non-intrusive inspection is key to maintaining the pace of 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)

Better technologies may permit more efficient cargo screening and examinations of a larger number of containers, ideally, prior to departing for and entering United States ports. Certainly, a continued focus on technology is appropriate. CBP is currently utilizing large-scale X-ray and gamma ray machines and radiation detection devices to scan cargo. The acquisition and deployment of radiation detection equipment is coordinated closely with DHS’ Domestic Nuclear Detection Office (DNDO). Presently, CBP operates over 913 radiation portal monitors (RPMs) at our Nation’s ports (including 342 RPMs at seaports), utilizes over 180 large scale non-intrusive inspection devices to examine cargo, and has issued 14,150 handheld-held radiation detection devices. DNDO is currently developing next-generation technologies for CBP and other operators that will provide improved detection capabilities. These next-generation systems will be gradually introduced at our nation’s ports beginning this calendar year. Also, over 600 canine detection teams capable of identifying narcotics, bulk currency, human beings, explosives, agricultural pests, and chemical weapons are deployed at our ports of entry. 158 Non-intrusive inspection devices are assuredly key to quick container examination. Equally important is the use of devices to detect intrusion into containers so that those containers passing inspection at the time of loading are not tampered with in route to the United States. In a perfect world such devices would detect the unauthorized intrusion anywhere on a container and not just intrusions through the container doors. “[J]ust because you have a device that secures the doors does not mean that the container is secure.” 159

#### Techonology solves

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 future of trade security will rely heavily on technology. There will never be enough human inspectors to look into every cargo container, truck, and rail car. Cargo cannot be guarded 24 hours a day. Technology promises to bridge the manpower gap by enabling the continual monitoring and tracking of freight. The use of electronics is already prevalent in commercial shipping. Cameras observe storage and loading areas at factories, ports, and warehouses. Digital identification cards restrict access to sensitive areas and store digital information about employees, including photographs, and increasingly, biometric data. Information about a cargo container’s contents is electronically transmitted to Customs officials before the container is even loaded onto a ship. Ironically, the single most visible element of the trading system—the cargo container— remains stubbornly low-tech and notoriously insecure. Indeed, instructions on how to break into a shipping container in under two minutes are readily available on the Internet.73 Most container seals currently in use are designed to detect intrusion, not stop it. Yet even in that limited role, many container seals are easily defeated.

#### Voluntary/Incentives Key

#### 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.

#### Private Solves

#### 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.

#### Fed Key

#### Federal Oversight is key to effective response

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)

Federal leadership needs to be unified “We need to overcome organizational inertia and conflicting agendas,” said one wargame participant. A single government focal point—be it a department or an offi cial—must be established to effectively deter and detect terrorist events, to oversee response and communications, and ensure economic recovery.

#### Only Customs Can Regulate

#### Customs controls Trade and is tasked with preventing terrorist weapons from entering the countery

**Widdowson** 2007 (Professor David Widdowson, the Chief Executive Officer of the Centre for Customs& Excise Studies at the University of Canberra, “THE CHANGING ROLE OF CUSTOMS:EVOLUTION OR REVOLUTION?”, World Customs Journal, <http://worldcustomsjournal.org/media/wcj/-2007/1/The_changing_role_of_Customs_evolution_or_revolution.pdf>)

As a direct result of 9/11, supply chain security now consumes regulatory thinking, and with this comes a real danger of focusing on tighter regulatory control at the expense of trade facilitation. In his address to Center for Strategic and International Studies on 17 January 2002, the then US Customs Commissioner, Robert Bonner said: Immediately following the terrorist attacks on September 11th, at about 10:05 a.m. on September 11, Customs went to a Level 1 alert across the country at all border entry points. Level 1 requires sustained, intensive anti-terrorist questioning, and includes increased inspections of travelers and goods at every port of entry. Because there is a continued terrorist threat, we remain at the Level 1 alert today. Shortly afterwards, the US Customs Container Security Initiative (CSI) and Customs- Trade Partnership Against Terrorism (C-TPAT) were announced. Primarily designed to protect global supply chains from concealment of terrorist weapons, these initiatives have had a sudden and major impact on the way in which customs and others involved in the international supply chain go about their business. The idea behind C-TPAT is for US Customs and Border Protection (CBP) to work with those involved in international trade to improve the security of their supply chains. The aim is to provide CBP with a method of identifying and focusing their resources on potentially high-risk consignments, that is, those that do not form part of a supply chain that is assessed to be ‘secure’. This approach – the need to focus on identifying both compliance and non-compliance – reflects a key element of contemporary compliance management, and is consistent with the provisions of the Revised Kyoto Convention. In this way, the C-TPAT program provides CBP with an opportunity to risk-manage its activities by assessing the integrity its C-TPAT partners’ supply chains, and in turn to provide those private sector partners with expedited processing and clearance.

#### Customs is responsible for facilitating trade and protect the US from terrorism

#### AllGov 2012 (AllGov.com, “[U.S. Customs and Border Protection](http://www.cbp.gov/)”, Everything our government really does, <http://www.allgov.com/agency/U_S__Customs_and_Border_Protection>)

United States Customs and Border Protection (CBP) is the unified border agency within the Department of Homeland Security (DHS). CBP employees manage, control and protect the nation’s border. CBP’s two main stated goals are anti-terrorism and facilitating legitimate trade and travel. CBP works to protect the U.S from acts of terrorism and reduce the vulnerability to the threat of terrorists through a multi-level inspection process. CBP is also responsible for preventing the transportation of drugs, illegal immigrants, traffickers, prohibited agricultural products and counterfeit goods, money, and intellectual goods across the border. CBP is made up of personnel who were formerly with the U.S customs, U.S Immigration, Animal and Plant Health Inspection Service and the entire U.S Border Patrol.

#### CBP is to oversee the flow trade while securing the border from potential threats

#### Department Of Homeland Security 6-21-2012 (Department of Homeland Security, “Written testimony of the U.S. Customs and Border Protection, U.S. Coast Guard, and U.S. Immigration and Customs Enforcement for a House Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management hearing titled “U.S.-Caribbean Border: Open Road for Drug Traffickers and Terrorists”, <http://www.dhs.gov/ynews/testimony/20120621-cbp-uscg-ice-caribbean-border-hsc.shtm>)

Our mission to promote homeland security and uphold public safety through the criminal and civil enforcement of Federal laws governing border control, customs, trade, and immigration. To do this, DHS has deployed a multi-layered, risk-based approach to enhance the security of our borders while facilitating the lawful flow of people and goods entering the United States. This layered approach to security reduces our reliance on any single point or program that could be compromised. It also extends our zone of security outward, ensuring that our physical border is not the first or last line of defense, but one of many. As America’s frontline border agency, CBP is responsible for securing America’s borders while facilitating legal travel and trade. Over the past three years, the Department of Homeland Security (DHS) has dedicated historic levels of personnel, technology, and resources in support of our border security efforts. The President’s Fiscal Year (FY) 2013 Budget Request continues these efforts by supporting the largest deployment of law enforcement officers to the frontline in our agency’s history: more than 21,000 Border Patrol agents, 1,200 Air and Marine agents, and 21,100 CBP officers, all who work 24/7 with state, local, tribal, and Federal law enforcement in targeting illicit networks trafficking in people, drugs, weapons, and money. Over the last year, we have brought greater unity to our enforcement efforts, expanded collaboration with other agencies, and improved response times.

Customs job is to regulate international trade and prevent illegal goods from being imported

CBP 2006 (U.S. Customs and Border Protection, “Importing into the United States: A Guide for Commercial Importers”, CBP.gov Publications, <http://www.cbp.gov/linkhandler/cgov/newsroom/publications/trade/iius.ctt/iius.pdf>)

Before September 11, 2001, the major responsibility of the former U.S. Customs Service was to administer the Tariff Act of 1930, as amended. When Customs subsequently merged with other border enforcement agencies to become U.S. Customs and Border Protection, CBP’s priority mission became homeland security: detecting, deterring and preventing terrorists and their weapons from entering the United States. This mission fits ideally with CBP’s long-established responsibilities for protecting and facilitating international trade. CBP retains its traditional enterprise of protecting the nation's revenue by assessing and collecting duties, taxes and fees incident to international traffic and trade. Further, by providing procedural guidance to the import community, CBP enhances and increases compliance with domestic and international customs laws and regulations. CBP thus helps importers assure that their shipments are free from terrorist or other malicious interference, tampering, or corruption of containers or commodities. Today, CBP is the nation’s premiere border enforcement agency, and it accomplishes this new mandate in part by executing the responsibilities for which it has always been known: controlling, regulating, and facilitating the movement of carriers, people, and commodities between the United States and other nations; protecting the American consumer and the environment against the introduction of hazardous, toxic or noxious products into the United States; protecting domestic industry and labor against unfair foreign competition; and detecting, interdicting, and investigating smuggling and other illegal practices aimed at illegally entering narcotics, drugs, contraband or other prohibited articles into the United States. CBP is also responsible for detecting, interdicting, and investigating fraudulent activities intended to avoid the payment of duties, taxes and fees, or activities meant to evade the legal requirements of international traffic and trade; and for detecting, interdicting, and investigating illegal international trafficking in arms, munitions, currency, and acts of terrorism at U.S. ports of entry.

### Organized Crime

#### Organized Crime

#### Container vulnerabilities are critical sources of income for organized crime

Global Security, 7/13/2011 (“Port Security Systems” http://www.globalsecurity.org/security/systems/ports.htm)

When first introduced, containers successfully reduced pilferage. Estimates indicated that during the early years of the container revolution, theft of containerized cargo dropped to less than one-tenth of 1 percent of all cargo shipped in containers. Unfortunately, after an initial honeymoon period, during which criminals adjusted to the new container system, other patterns of theft developed. Organized crime recognized the potential for big business. Containers, stacked in terminals, could be stolen as a whole, opened and made subject to pilferage, or serve as a conduit for drug smuggling. Much larger 'packages' containing higher value cargoes could now be spirited away with comparative ease and the spoils made it worth using more elaborate methods of deception and daring. Whereas, previously ten televisions might go missing because that was all thieves could carry or secrete, now two hundred could be stolen at a go in a container. For example, computer laptops, cellular telephones, perfume, and wearing apparel are among the top items stolen and could be worth from hundreds of thousands of dollars to millions of dollars per container load. A pallet of these devices can command upwards of $250,000. Sixty-four pallets can be loaded into a single 40-foot container, with a net value of $16 million. Based on new patterns of cargo theft, the US Coast Guard, the NCSC, and American Trucking Association (ATA) estimate that the value of single cargo thefts is on the rise, averaging approximately $500,000 in 1996. This estimate represents a five-fold increase from 1970. Containerized cargo theft is carried out primarily as an organized criminal conspiracy. Substantial evidence supports the hypothesis that most theft of containerized cargo is systematic in method. Often, criminals act with apparent information about cargo manifests, suggesting that collusion is occurring with transportation employees. Cargo terminals are particularly vulnerable to employee penetration at intermodal transfer points, warehouses, rail yards, and docks. In its Ports of the World: A Guide to Cargo Loss Control, the CIGNA Corporation reports that the majority of cargo loss claims involve cargo taken from transportation facilities by personnel authorized to be there and on vehicles controlled or similarly authorized by management. This immense network of importers, wholesalers, freight brokers, truckers, and dock workers create problems for law enforcement and transportation operations in pinpointing instances of bribery, extortion, or "purchased" information. Estimates indicate that well over 80 percent of all theft and pilferage of transportation cargoes is accomplished by, or with the collusion of, persons whose employment entitles them access to the cargo that is stolen. Each year, cargo thefts from terminals (including ports, docks, intermodal facilities, rail yards, warehouses, transfer facilities), motor carriers, and maritime vessels account for between $3.5 billion (conservative FBI estimate) to more than $10 billion (NCSC estimate) in lost merchandise. This figure represents a significant portion (3.1 percent) of annual surface transportation general freight revenue. Indirect costs related to cargo theft (not including all law enforcement or security technology costs) range from $20 billion to $60 billion each year. The growing volume of containerized trade provides numerous opportunities for smuggling illicit drugs. Containers sealed in one nation may not be opened until they reach a final destination in another. Both the volume of container trade and the labor-intensive methods required for inspecting containers, severely limit law enforcement personnel and freight transportation operators in identifying and preventing drug smuggling. The Drug Enforcement Agency (DEA) reports that the use of legitimate commercial freight containers by smugglers to conceal cocaine and heroin shipments has become a large-scale problem compromising the operations of legitimate business enterprises. Victimized companies are sustaining significant financial loss, erosion of operating integrity, and diminished corporate reputation. One self-insured trucking company noted that in the second quarter of this year (1998) it had a container stolen from its facility valued at approximately $3 million. Further, since concealment of illegal narcotics in commercial shipping is the primary method for transporting drugs and money into and out of the United States, organized crime has intensified involvement in the transportation sector. Corporations financed by drug profits may purchase, own, and operate apparently legitimate trucking companies and transportation operations to transport products and to obtain crucial shipping information. Organized criminal groups are also successfully infiltrating the transportation industry by compromising employees into acts of commission using bribery or extortion to induce collusion. In addition to transportation employees, police, customs and other government officials have been targeted for corruption.

#### Ports Are Key

#### Ports ships are key to Drug Cartels to smuggle drugs into the country

DEA 04 (Drug Enforcement Agency, Government agency, May 2004, “Drug Trafficking in the United States”, Almanac of Policy Issues, <http://www.policyalmanac.org/crime/archive/drug_trafficking.shtml>)

The illegal drug market in the United States is one of the most profitable in the world. As such, it attracts the most ruthless, sophisticated, and aggressive drug traffickers. Drug law enforcement agencies face an enormous challenge in protecting the country's borders. Each year, according to the U.S. Customs Service, 60 million people enter the United States on more than 675,000 commercial and private flights. Another 6 million [people] come by sea and 370 million by land. In addition, 116 million vehicles cross the land borders with Canada and Mexico. More than 90,000 merchant and passenger ships dock at U.S. ports. These ships carry more than 9 million shipping containers and 400 million tons of cargo. Another 157,000 smaller vessels visit our many coastal towns. Amid this voluminous trade, drug traffickers conceal cocaine, heroin, marijuana, MDMA, and methamphetamine shipments for distribution in U.S. neighborhoods.

#### Drugs Key

#### **Demand drives production – US demand very large**

President’s Commission on Organized Crime, 2009 (“America’s Habit: Drug Abuse, Drug Trafficking & Organized Crime,” Schaffer Library of Drug Policy, <http://www.druglibrary.org/schaffer/govpubs/amhab/amhabc7.htm>)

A clear example of the relationship of supply and demand is provided by the case of heroin trafficker Cecily Lermusiaux, who with several associates, moved heroin into an area of Las Vegas where its use among "middle to high-class whites" was previously unknown. In a scheme which began with the distribution of free samples of heroin, Lermusiaux's independent heroin business generated a profit of several million dollars in approximately six years. The demand for drugs is also widely recognized as the fuel that the illicit drug industry needs to operate. According to Colombian President Belisario Bentancur: In the world war against narcotics, we need the commitment of the consumer nations to attack the traffic with the same vigor we have shown. We can make all the sacrifices possible, but if there is enormous demand, production will never be completely eradicated. This sentiment has been echoed by the other side of the law. Carlos Lehder, who heads one of Colombia's most notorious cocaine cartels, sees the American demand for drugs as the driving force behind the "bonanza" of drug trafficking: The demand for drugs in the United States is so great that the producer countries like Colombia play a really tiny role compared to the total consumption of the United States.

#### US attracts drug traffickers

US Drug Enforcement Agency ’04 (Us Drug Enforcement Agency. “Drug Trafficking in the United States.” United States Drug Enforcement Administration. http://www.justice.gov/dea/concern/drug\_trafficking.html)

The illegal drug market in the United States is one of the most profitable in the world. As such, it attracts the most ruthless, sophisticated, and aggressive drug traffickers. Drug law enforcement agencies face an enormous challenge in protecting the country's borders. Each year, according to the U.S. Customs Service, 60 million people enter the United States on more than 675,000 commercial and private flights. Another 6 million come by sea and 370 million by land. In addition, 116 million vehicles cross the land borders with Canada and Mexico. More than 90,000 merchant and passenger ships dock at U.S. ports. These ships carry more than 9 million shipping containers and 400 million tons of cargo. Another 157,000 smaller vessels visit our many coastal towns. Amid this voluminous trade, drug traffickers conceal cocaine, heroin, marijuana, MDMA, and methamphetamine shipments for distribution in U.S. neighborhoods.

#### The US is a profitable market for drug traffickers

Klenowski ’11 (Paul M. Klenowski. Paul Klenowski works in the Department of Criminology at the Indiana University of Pennsylvania, focusing on the motivations of white collar criminals. “Drug Trafficking.” Encyclopedia of Immigration. http://immigration-online.org/466-drug-trafficking.html)

Definition: Importation and sale of narcotic and other drugs legally defined as controlled substances Significance: Drug trafficking and immigration are strongly correlated because most of the illegal drugs that enter the United States originate outside the country. Thousands of undocumented immigrants from various countries work as couriers, smuggling narcotic and other banned drugs into the United States. The drug trade in illegal drugs began reaching epidemic proportions during the 1990’s. Scholars have estimated that profits from international drug trafficking were nearing $10 trillion dollars annually by the twenty-first century. The United States is meanwhile the most lucrative market for international drug traffickers, with tons of illegal drugs smuggled into the country every day. Many of the couriers who are paid to bring in the drugs are themselves illegal immigrants. Illegal drug trafficking has become a global black market consisting of the farming, processing, distribution, and sale of illegal narcotics. Most countries throughout the world prohibit trade, except under license, of many types of illegal drugs. The illicit drug trade operates much like other illegal underground markets. Drug gangs and cartels specialize in the separate processes along the supply chain, sometimes involving multiple countries. The cartels vary in size, ethnic and racial membership, organizational structure, and country of origin. Supply chains range from low-level street dealers to mid-level street gangs and couriers, up to multinational drug empires. Illegal drugs can be grown and processed almost anywhere: in the wilderness, on farms and plantations, in residential gardens, inside residential homes, and in labs secreted inside such structures as abandoned city buildings in major urban districts or rural mobile home parks. The most common element connecting these places of production is that all the locations must remain secret to avoid detection by law enforcement. Much of the twenty-first century illegal drug cultivation and processing takes place in developing nations; however, some is done in such developed nations as the United States, Canada, Germany, and France. Consumption of illegal drugs is widespread globally and has been regarded as having reached epidemic proportions within the United States.

#### Armed Conflict Impact

#### Transnational organized crime fuels global armed conflict.

Cockayne, 07. (John Cockayne, Associate at International Peace Academy (IPA) since March 2006. Before joining IPA, he served as Director of the Transnational Crime and Extradition Units in the Australian Attorney-General’s Department, was a Graduate Scholar at the Institute for International Law and Justice at New York University School of Law, and worked at the International Criminal Tribunal for Rwanda, the Special Court for Sierra Leone, and in private legal practice in Sydney and Paris. Mr. Cockayne is Chair of the Editorial Committee of the Journal of International Criminal Justice, “Transnational Organized Crime: Multilateral Responses to a Rising Threat”, International Peace Academy)

Strong anecdotal evidence suggests that armed conflict is fueled or perpetuated by the presence of TOC networks, which allow armed groups to sell locally-acquired resources on global markets.34 Moreover, the apparent “convergence” of armed conflict and OC in many theaters has led many theorists to argue that the traditional distinction between the two needs to be reconsidered.35Yet such an approach is problematic: it risks conflating divergent phenomena, producing poorly calibrated policy responses; it risks leading to the abandonment of existing analytical and legal frameworks, jeopardizing the safeguards associated with each; and at present, such basic questions as the impact of the presence of different types of TOC on the onset, duration, and termination of armed conflict remain unanswered. At present, existing analysis seems to support only three broad hypotheses about the relationship between OC strategy and the dynamics of armed conflict and related forms of political violence. First, armed conflict is in some cases the result of a violent struggle between predatory OC and a state. Predatory OC groups may find it convenient to be cloaked as political movements, as has arguably occurred in Sierra Leone, Liberia, Burma, Colombia, and DRC. Predatory OC may contest territorial control, even capturing effective control of a small territory from the state and creating “statelets.”36 We know little about what types of functional weakness make states vulnerable to predatory OC producing armed conflict;37 but it does appear that in such cases, TOC may prolong conflict by providing external sources of inputs such as finance, materiel, and personnel. This brings us to a second relationship between TOC and political violence: where TOC is the byproduct of armed conflict or other forms of political violence (rather than armed conflict being the byproduct of OC, as is the case in the first scenario). As Peter Andreas has noted, in today’s globalized economy, “[m]ilitary success on the battlefield can significantly depend on entrepreneurial success in the illicit economy.”38 There are numerous examples of armed groups resorting to smuggling to finance violence—e.g., of narcotics (KLA, PKK, Islamic Movement of Uzbekistan, Taliban, and Colombian, Peruvian, Burmese and Nepalese armed groups); cigarettes (Hizbullah, Northern Irish paramilitaries); or natural resources (Colombia, Burma, Liberia, Sierra Leone, Angola, Nigeria, DRC, Iraq). In such cases, there may be significant economic cooperation between competing groups.39 This points to a commercialization of war,40 the emergence of “warlordism,” and the institutionalization of violent criminal disorder as a shadow economic system, carried out through large-scale criminal enterprises connecting local and global markets.41 That would also suggest that the presence of TOC groups risks prolonging (and perhaps accelerating the resort to) armed conflict. But again, reliable empirical analysis remains thin. Third, armed conflict—or similar, but lower level violence—may result from violent competition between OC groups, particularly those adopting symbiotic or parasitic, rather than predatory, strategies.

#### Corruption

#### Transnational organized crime corrupts all aspect of the global system.

Cockayne, 07. (John Cockayne, Associate at International Peace Academy (IPA) since March 2006. Before joining IPA, he served as Director of the Transnational Crime and Extradition Units in the Australian Attorney-General’s Department, was a Graduate Scholar at the Institute for International Law and Justice at New York University School of Law, and worked at the International Criminal Tribunal for Rwanda, the Special Court for Sierra Leone, and in private legal practice in Sydney and Paris. Mr. Cockayne is Chair of the Editorial Committee of the Journal of International Criminal Justice, “Transnational Organized Crime: Multilateral Responses to a Rising Threat”, International Peace Academy)

All organized crime (OC) is clandestine, hiding in the dark “shadows,”5 because OC substitutes might for right, and coercion for capital. Transnational organized crime (TOC) uses the shadowy “sovereign-free” areas of the international system, where state control is weak or ineffective—such as war zones, cyberspace and private bank accounts—to operate.6 Operating in such zones beyond the reach of state-based crime control, TOC slowly corrupts and undermines state, social and global systems of governance. The growth of TOC undermines social, state and international controls on a range of public ills from political and economic violence to corruption, and from environmental harm to disease. As the violent forms of authority buttressed by OC corrupt and penetrate state, social and international institutions, gaining increasing control over territory, markets and populations, we risk not only a crisis of state and international institutions, but also institutionalizing crisis.

#### Laundry List

#### Transnational crime undermines all aspects of society.

Shelley, 95. (Louise Shelley, Professor in the Department of Justice, Law, and Society and the School of International Service at American University and founder and Director of the Transnational Crime and Corruption Center (TraCCC), Transnational organized crime: An imminent threat to the nation-state, Journal of International Affairs.)

The costs of transnational organized crime are not exclusively monetary. Transnational organized crime undermines political structures, the world economy and the social order of the countries in which the international crime groups are based and operate. The resulting instability invites more crime, and may preclude the institutionalization of democratic institutions, the rule of law and legitimate markets. Transnational organized crime undermines civil society and human rights. Through intimidation and assassination of journalists in different countries, it limits freedom of the press and individual expression. Transnational organized crime also undermines the creation of civil society by dominating independent philanthropic organizations and by intimidating citizens in movements that challenge organized crime[9] The infiltration of these groups into labor unions violates citizen labor rights. International trafficking in prostitution and pornography demeans both women and children, and the illegal smuggling of individuals to work in situations where they are often exploited raises serious human rights concerns.

#### Democracy

#### International organized crime kills democracy promotion

Shelley, 95. (Louise Shelley, Professor in the Department of Justice, Law, and Society and the School of International Service at American University and founder and Director of the Transnational Crime and Corruption Center (TraCCC), Transnational organized crime: An imminent threat to the nation-state, Journal of International Affairs.)

The world political order becomes increasingly stable when more nations establish democratic forms of government based on respect for the rule of law and government through consensus. International organized crime is detrimental to existing democracies and to societies in transition to democracy. Transnational crime undermines the rule of law and the legitimacy of democratic government through its corruption of individuals and the judicial process. Organized crime groups often supplant the state in societies undergoing a transition to democracy, as their representatives assume key positions in the incipient legislatures, which are responsible for crafting the new legal framework for the society. Their presence within legitimate state institutions undermines political stability because their goals are to further their own criminal interests (illicit profits), not the interests of the populace at large. Transnational organized crime groups in both developed and developing democracies seek to corrupt high-level government officials both on the groups' home tuff and in the countries where they operate. But these groups are often more successful when their efforts are conducted in nation-states that are in political transition, because the controls over the legal process do not yet function as they do in a stable democracy.

#### Proliferation

#### Transnational organized crime causes clandestine proliferation

Shelley, 95. (Louise Shelley, Professor in the Department of Justice, Law, and Society and the School of International Service at American University and founder and Director of the Transnational Crime and Corruption Center (TraCCC), Transnational organized crime: An imminent threat to the nation-state, Journal of International Affairs.)

Transnational organized crime groups also threaten states through their trafficking in nuclear materials. Now the world no longer worries about nuclear conflict between the world's superpowers. Instead, today the nuclear threat comes largely from the arms trafficking of organized crime, a new and highly pernicious form of illicit activity. The smuggling of nuclear materials may enable some country or crime group to independently produce a nuclear weapon, therefore raising the potential for nuclear blackmail. Traditional scholarship applies the concept of the criminalized state to Nazi Germany. Yet it is equally valid to apply the term to a state apparatus used to further the goals of organized crime groups This is evident in Italy where, for more than a century, a symbiotic relationship has existed between crime and politics[10].

#### Economy

#### Transnational organized crime impacts the world economy negatively.

Shelley, 95. (Louise Shelley, Professor in the Department of Justice, Law, and Society and the School of International Service at American University and founder and Director of the Transnational Crime and Corruption Center (TraCCC), Transnational organized crime: An imminent threat to the nation-state, Journal of International Affairs.)

The impact of international organized crime groups on the world economic order is equally disturbing. Much has been written about the pernicious effects of multinational corporations that transfer operations outside their domestic base, often in order to elude domestic legal controls. A typical critique concludes that their "exploitative effects on rich and poor nations remain unchecked." [14] International law lacks the legal enforcement power necessary to control the behavior of such international corporations. The innate obstacles to regulating the abuses of multinationals (i.e., the diversity of laws among nations, the lack of extradition treaties and the desire of developing nations to attract foreign capital at any cost) are only amplified when replaced by illicit multinationals -- transnational organized crime. The practice by transnational criminal organizations of large-scale money laundering, of corrupting of key officials in economic and customs positions and of utilizing banks, stock exchanges, venture capital opportunities and commodities markets, all undermine the financial security of world markets. The pensions and savings of ordinary citizens are also jeopardized when banks and stock funds collapse because of illegal manipulation of the financial sectors by international organized crime groups. The BCCI affair may be the most notable of these scandals, as its fallout affected citizens in many different countries. But BCCI is unique only in its complexity, the scale of its losses and the fact that it was uncovered, not in its occurrence.[15]

#### Terrorism

#### **Organized Crime is a major threat to US- help fund terrorist activities**

Finklea 2010 (Kristin M. Finklea, Analyst in Domestic Security, “Organized Crime in the United States: Trends and Issues for Congress”, Federation of American Scientists, <http://www.fas.org/sgp/crs/misc/R40525.pdf>)

Organized crime threatens multiple facets of the United States, including the economy and national security. In fact, the Organized Crime Council was reconvened for the first time in 15 years to address this continued threat. Organized crime has taken on an increasingly transnational nature, and with more open borders and the expansion of the Internet, criminals endanger the United States not only from within the borders, but beyond. Threats come from a variety of criminal organizations, including Russian, Asian, Italian, Balkan, Middle Eastern, and African syndicates. Policymakers may question whether the tools they have provided the federal government to combat organized crime are still effective for countering today’s evolving risks. Organized crime could weaken the economy with illegal activities (such as cigarette trafficking and tax evasion scams) that result in a loss of tax revenue for state and federal governments. This is particularly of issue given the current state of the country’s economic health. Fraudulent activities in domains such as strategic commodities, credit, insurance, stocks, securities and investments could further weaken the already-troubled financial market. On the national security front, experts and policymakers have expressed concern over a possible nexus between organized crime and terrorism. Despite the difference in motivation for organized crime (profit) and terrorism (ideology), the linking element for the two is money. Terrorists may potentially obtain funding for their operations from partnering directly with organized crime groups or modeling their profitable criminal acts. Even if organized crime groups and terrorist organizations do not form long-term alliances, the possibility of short-term business alliances may be of concern to policymakers.

### Answers to Offcase Positions

#### Plan Popular

#### Plan is popular – Viewed as anti-terrorism

Lane, Colonel US Army 2/4/2009 (Drefus Sr. “U.S. SEAPORT SECURITY: CRITICAL CHALLENGE FOR DEPARTMENT OF HOMELAND SECURITY” USAWC STRATEGY RESEARCH PROJECT <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA499287>)

The 9/11 terrorist attack on the World Trade Center in New York and on the Pentagon instantly created a new American consciousness of the homeland’s vulnerability to terrorism. Political will rose to an unprecedented level to address the nation’s new priority of protecting the homeland. In the aftermath of 9/11, the President then created the Department of Homeland Security to develop and implement a comprehensive national strategy for homeland security. The 2004 Presidential Directive for Maritime Security Policy mandated that the collaboration between state, local, and private sector entities be conducted at the federal level to achieve complete and unified maritime security programs and initiatives. 1 Thus, U.S. seaports have been designated vital to the US economy and national security strategy. The maritime transportation system was identified as an easy target as a result of the 9/11 commissions investigations. Seaports were considered to be the most vulnerable sectors that could affect U.S. economy. 2 This SRP contributes to port security awareness of maritime programs by providing a preliminary assessment of U.S. seaports security.

#### Bipartisan support for port security

SDN 11 (Security Director Network; covers the news, trends and ideas relevant to end users in the security profession; “New Congressional group to support port security”; SDN; http://www.securitydirectornews.com/public-sector/new-congressional-group-support-port-security)

Two members of Congress last week created a new bipartisan caucus to promote the growth and security of the United States' 350 commercial sea and river ports. Rep. Janice Hahn (D-CA) and Rep. Ted Poe (R-TX) announced on Oct. 25 the formation of the bipartisan House Ports Opportunity, Renewal, Trade, and Security (PORTS) Caucus, according to a press release. U.S. ports support 13.3 million jobs and account for $3.15 trillion in business activity to the economy. “Promoting and protecting our nation’s ports is critical to both national security and economic security,” Rep. Poe said in a statement. “Ports are the gateway in and out of the United States. They are our country’s link to the rest of the world and the global economy.” The United States is home to more than 350 commercial sea and river ports that support 3,200 cargo and passenger handling facilities, according to the release. Each day, U.S. ports move both imports and exports totaling some $3.8 billion worth of goods through all 50 states. Additionally, ports move 99.4 percent of overseas cargo volume by weight and generate $3.95 trillion in international trade. “Ports are a critical piece of our nation's economic infrastructure,” Geraldine Knatz, executive director of the Port of Los Angeles, said in a statement. “Maintaining secure, reliable and efficient seaports will generate much needed jobs and make American businesses more competitive abroad.”

#### Plan Unpopular

#### GOP doesn’t like port security

Legum, 06 (Judd, Correspondent for ThinkProgress Security, “Right-Wing Blocks Funding For Port Security, Disaster Preparedness,” Think Progress, <http://thinkprogress.org/security/2006/03/16/4272/port-security-funding/>)

Moments ago, the House of Representatives narrowly defeated an amendment proposed by Rep. Martin Sabo (D-MN) that would have provided $1.25 billion in desperately needed funding for port security and disaster preparedness. The Sabo amendment included: – **$300 million to enable U.S. customs agents to inspect high-risk containers at all 140 overseas ports** that ship directly to the United States. Current funding only allows U.S. customs agents to operate at 43 of these ports. – **$400 million to place radiation monitors at all U.S. ports of entry**. Currently, less than half of U.S. ports have radiation monitors. – **$300 million to provide backup emergency communications equipment for the Gulf Coast**. Meanwhile, the Bush budget – which most of the members who voted against this bill will likely support – contains an increase of [$1.7 billion for missile defense](http://images1.americanprogress.org/il80web20037/ThinkProgress/2006/supp.doc), a program that doesn’t even work.

#### **Cost and needed technology makes increasing port security unpopular**

Schneidmiller2/9/ 2012 (Chris Schneidmiller, Chris Schneidmiller has been editor of Global Security Newswire since April 2009, after serving for more than five years as deputy editor. He leads a team of four journalists that provides original reporting and aggregation on global issues of nonproliferation and weapons of mass destruction.  Prior to his time at GSN, Schneidmiller spent 10 years as a reporter and editor for several daily newspapers, most recently at the former Journal Newspapers Co. near Washington, D.C. He has received several awards for news and feature reporting, and is a graduate of the University of Texas at Austin, “Homeland Security to Extend Cargo Nuclear Scanning Deadline,” Global Security Newswire, <http://www.nationaljournal.com/reporters/bio/92>)

WASHINGTON -- The Homeland Security Department does not appear to be trying to meet a congressional mandate that by July all U.S.-bound cargo be scanned for weapon-usable radioactive materials before leaving foreign seaports, a senior congressional investigator said on Tuesday (see GSN, Dec. 3, 2009). Instead, the agency anticipates it will extend the deadline for all ports to be ready by July 2014, Stephen Caldwell, a maritime security specialist with the Government Accountability Office, said in a prepared statement to a House subcommittee. Department officials acknowledged in their own written testimony to the panel that only one port is participating in a pilot program to test the viability of the requirement, even though six docks were earlier expected to take part. They made no mention of a deadline extension, but Homeland Security Secretary Janet Napolitano has made it clear in previous comments that one is in the offing. The officials did highlight complications to be overcome and the billions of dollars necessary to put the full-scope program into place. “Have you given up on 100 percent screening?” Representative Sheila Jackson Lee (D-Texas) asked during a hearing of the House Homeland Security Border and Maritime Security Subcommittee. “We are continuing to operate under the law,” responded David Heyman, assistant Homeland Security secretary for policy. Lawmakers acknowledged the difficulty or potential impossibility of covering the roughly 700 ports that ship cargo directly to the United States. Some, nonetheless, made it clear they are not satisfied by the current situation. Homeland Security “has failed to make an honest effort to implement the mandate,” said Representative Bennie Thompson (D-Miss.), a leading backer of the measure. “We’ve heard a litany of reasons that 100 percent scanning cannot or should not be done. … Of course, the surest way to fail is not to try at all.” The potential for terrorists to use the global shipping system to smuggle a nuclear or radiological weapon into the United States is one of many threats the Bush and Obama administrations have sought to address in the years since the Sept. 11 attacks. A nuclear strike on the country is considered a low probability but high impact event, with the potential to cause devastating human and economic costs. The Sept. 11 Commission law passed by Congress in 2007 set a July 1, 2012, deadline after which no cargo container would be allowed to enter the United States unless it had been checked by radiation detection and nonintrusive imaging technology. The law allowed for extensions of the mandate in two-year increments, accompanied by advanced notification to Congress. Roughly 5 percent of cargo containers undergo the demanded physical scanning today either at the foreign port of departure or upon arrival in the United States, according Kevin McAleenan, acting assistant commissioner for field operations at DHS Customs and Border Protection. One lawmaker who pressed for inclusion of the screening measure in the legislation said scanning containers overseas is crucial to ensuring the United States is protected against cargo-carried weapons. Catching a nuclear bomb at a U.S. port “may very well be too late,” said Representative Jerrold Nadler (D-N.Y.). “Reading the cargo manifest is not enough. Trusting certain shippers is not enough,” he testified during the hearing on global supply chain security. “We must verify the contents of the containers at the point of origin, before they are loaded on a ship bound for America. And so the law is designed to do just that.” The SAFE Port Act approved in 2006 called for a pilot program to determine whether 100 percent scanning could be reasonably implemented. The Homeland Security and Energy departments in December of that year launched the Secure Freight Initiative, which deployed technology to ports in Honduras, Hong Kong, Oman, Pakistan, South Korea and the United Kingdom. None of the test ports were able to scan all U.S.-bound cargo, putting into question the viability of the congressional demand for 100 percent screening, Caldwell said. While relatively “low-volume” sites in Honduras, Pakistan and the United Kingdom checked most containers heading to the United States, busier shipping sites in Hong Kong and South Korea scanned only about 5 percent of the cargo, he stated. Both Caldwell and the Homeland Security officials identified a number of issues that hampered the test program, including safety worries, malfunctioning scanning technology and inferior images. The Sept. 11 act also failed to specify who could lead the scanning efforts at foreign ports and who would provide funding for the technology and scanning activities under the 100 percent demand, the GAO official said. While the U.S. Congressional Budget Office assessed early on that foreign governments or port operators would bear the cost of the program, Customs and Border Protection said it was not clear that other governments would accept those terms, Caldwell told Global Security Newswire on Thursday. The Homeland Security branch “documented numerous challenges associated with implementing 100 percent scanning including diplomatic challenges, international trade opposition, the need for port reconfiguration, potential for reciprocal requirements on the United States, and lack of available technology to efficiently scan transshipped cargo,” according to a joint statement to the subcommittee from McAleenan, Heyman and Coast Guard Rear Adm. Paul Zukunft.

#### Perm (Many CPs)

#### Perm Solves - Combination of approaches 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)

The lesson to be learned from recent developments in securing shipping containers is that there is no one solution – no single answer. The answers lie in what the government seems to have realized: it is a number of complementary approaches, used together, that provides the best method of protection. Resisting the temptation to rely on a single, all-encompassing solution is most likely to prevent unacceptable economic results, and most likely to keep our enemies guessing and prevented from undermining our security.

#### A2: States CP

#### Grants cut by massive amounts, states cannot perform necessary assessments.

Bennett 05-18-12 (John C.W. Bennett, Principle Nature of Business: Education / Research / Training Professional Interests: Maritime Regulations and standards, Offshore Drilling, Offshore Oil / Gas Exploration, Offshore Structures, Port Authority Security Services & Systems, Vessels, “Comments from the Public”, Maritime Professional, http://www.maritimeprofessional.com/Blogs/Maritime-Transportation-Security-News-and-Views/May-2012/NMSAC-May-2012-Meeting-%E2%80%93-Part-1.aspx)

A representative of the American Association of Port Authorities (AAPA) expressed the AAPA’s concerns for the future of Port Security Grants under the proposal to combine all DHS grant programs into one and urged NMSAC to recommend to the DHS Secretary that Port Security Grants be kept as a separate program. The AAPA fears that the States are not in a position to figure out port security and are not likely to give ports a fair share of the overall total. The AAPA was disappointed by the handling of DHS grant programs this year, where Congress cut the combined programs by 40% and left it up to the Secretary to parcel the money between the various programs. Rather than 40%, Port Security Grants were cut by 58%. One major need that will become apparent over the next few years is the replacement of radiation portal monitors as they grow old. Asked by a NMSAC member why the AAPA didn’t think the States would fund port needs, the Association representative opined that, faced with a smaller pot of funding, the States would fund what they knew and were familiar with. Additionally, the States weren’t equipped to perform port risk/security assessments, unlike the Area Maritime Security Committees in the current program.

#### A2: Topicality Investment

#### **Grants are a form of Investment**

World Bank, 4-18-12 (The World Bank Institute (WBI) is a global connector of knowledge, learning and innovation for poverty reduction, “Investment, Development Policy ad Program-for-Results Operations,” [http://web.worldbank.org/WBSITE/EXTERNAL/PROJECTS/0,,contentMDK:20120732~menuPK:268725~pagePK:41367~piPK:51533~theSitePK:40941,00.html](http://web.worldbank.org/WBSITE/EXTERNAL/PROJECTS/0%2C%2CcontentMDK%3A20120732~menuPK%3A268725~pagePK%3A41367~piPK%3A51533~theSitePK%3A40941%2C00.html))

The World Bank funds three basic types of operations: investment operations, development policy operations, and Program-for-Results operations. Investment operations provide funding (in the form of IBRD loans or IDA credits and grants) to governments to cover specific expenditures related to economic and social development projects in a broad range of sectors. Development Policy operations provide untied, direct budget support to governments for policy and institutional reforms aimed at achieving a set of specific development results. Program-for-Results operations support the performance of government programs by strengthening institutions and building capacity. The instrument links the disbursement of funds directly to the delivery of defined results.

## RFID’s Solvency - Mechanism

### Solvency

#### General

#### RFIDs are effective – they do not require power

Benin, 4/13/2004 (Joseph, “Radio Frequency Identification (RFID) Tags & Their Implication to Container Security” International Security Seminar Sam Nunn Security Program)

In order to understand how RFID tags can be implemented for use in any given application, including container security, it is important to also know some of their key features. While at their most basic level RFIDs are glamorized barcodes, the fact is that they contain capabilities an order of magnitude greater than their black and white predecessors. In the end, RFID has the potential to revolutionize how processes are managed, businesses are operated, and even inspire new automated solutions [5]. Line of Sight RFIDs do not require a clear line of sight between the tag and reader. They can be read, depending on signal strength and environmental conditions, through all manner of boundaries including plastic, water, and metals. Robustness The fact that RFIDs do not need to be in plain view allows them to be placed in hardened cases. This provides for greater robustness within the device as well as more ideal placements that are less likely to be scraped or subject to shock. This results in high reliability rates, even in the harshest of environments. Read Characteristics The time it takes to process labeled goods is drastically reduced since an RFID reader can scan multiple tags simultaneously and from greater distances,. This enables tracking of individual items; not just pallets or boxes. This eliminates manual data entry and the corresponding delays and errors introduced.

#### RFID tags increase security and efficiency

Tsai 12-7-07 (Louis Tsai, Part of the University of California, Mechanical and Aerospace Engineering Department, “Container Tracking with RFID and Port Security”, WINMEC, <http://www.winmec.ucla.edu/rfid/course/2007f/Container%20Tracking%20with%20RFID%20and%20Port%20Security.pdf>)

Millions of cargo containers enter the U.S. borders annually. The Port of Long Beach and Port of Los Angeles, located in Southern California, are two major ports in the United States. On a daily average, it is possible for one port to handle up to 30,000 cargo containers. Unfortunately, less than ten percent of cargo containers are ever inspected by U.S. Customs. Ideally, all cargo containers should be opened and inspected. However, if every cargo container were to be inspected, it would lead to massive bottleneck due to the limited amount of resources for that endeavor. This is one of the main reasons only a small percentage of cargo containers are ever inspected. One idea to ameliorate this issue of security and efficiency has involved the incorporation of RFID technology into shipping ports. There are many applications to shipping ports including attaching RFID tags to port employees. Using RFID, the port can monitor whether an individual has entered a secure portion of the port, or an area where they are not permitted1. Another proposal are, RFID tags temporarily attached to trucks that enter the ports. For example, Port of Oakland has begun attaching RFID tags to trucks entering its premises. The goal is to automate security, shorten truck waits at the gate and increase the visibility of truck traffic within the port2. Container tracking is another option for the use of RFID technology. The focus of this research will center on how RFID tags on containers can improve security and increase efficiency at the Port of Long Beach. RFID has already proven its capability of increasing efficiency within the terminals by speeding the gate check process and provide real-time location of tens of thousands of containers stacked in yards3. With the possibility of incorporating sensors to add an extra layer of security, this may greatly improve the overall operation of the port.

#### RFID will be more sufficient than previous tags, solves all current problems.

Mullen n.d.-n.d.-07 (Dan Mullen, President of AIM Global, “The application of RFID technology in

a Port”, AIM Global, <http://www.aimglobal.org/technologies/rfid/resources/porttech.pdf>)

While there has been an ISO standard for tagging of maritime containers for a number of years, few container owners have implemented tagging; primarily because tag costs were initially very high. A new generation of active tags, however, has brought the cost down considerably, making it more feasible to tag the tens of thousands of containers in use. A continuing problem with intermodal containers is the presence of multiple identification numbers on many containers. There may be one number on the side and another number on the end – and terminal operators have little guidance as to which is correct. The increased concerns over the possible use of maritime shipping containers as a means of entry for illegal immigration, weapons, and chemical or biological agents means that positive identification of each container, under SST and CSI, will only increase. RFID tags provide a secure answer to this requirement. Readers placed on gantries and yard vehicles will be able to automatically record the identity of each container as it’s offloaded and transported within the terminal.

#### RFID reduce losses and labor, tracking is automated and accurate.

ZTC 06-n.d.-07 (Zebra Technologies Corporation, Zebra Technologies is a global leader in barcode and label printing solutions including printers, RFID, supplies, software and RTLS, “Managing Shipping Containers with RFID”, Zebra Technologies Corporation, <http://www.zebra.com/podcasts/rfid_executive_summaries/ES14368L_ContainerMgmt.pdf>)

Because RFID operations are proven to reduce losses and labor. It's very cost-effective to apply RFID smart labels to permanently identify and track expensive shipping containers. With RFID, reusable shipping containers can be automatically identified and added or removed from the asset pool database each time they enter or leave your facility. Readers can be built into dock doors, forklifts and mobile computers to support a variety of material handling processes. No labor time is needed to record serial numbers at the shipping and receiving dock or warehouse, or to enter them into the computer system. Tracking is automated, accurate and complete, leading to improved asset visibility and utilization. Because RFID is standardized and compatible with legacy systems. Companies don't have to radically redevelop their databases or asset management applications to take advantage of RFID. Legacy serial numbers plus standardized, commonly used identifiers such as Global Returnable Asset Identifiers (GRAIs) and Serial Shipping Container Codes (SSCCs) can be encoded into RFID tags, and also printed as bar codes to complement legacy operations. There are also several widely supported RFID technology standards suitable for identifying logistics containers, including the EPCglobal Gen 2 and ISO 18000 standards, plus real time locating systems (RTLS) technology that is standardized and is also compatible with legacy Wi-Fi® wireless networks.

#### Increases Efficiency

#### An investment in RFID will allow for improved security and efficiency.

Tsai 12-7-07 (Louis Tsai, Part of the University of California, Mechanical and Aerospace Engineering Department, “Container Tracking with RFID and Port Security”, WINMEC, <http://www.winmec.ucla.edu/rfid/course/2007f/Container%20Tracking%20with%20RFID%20and%20Port%20Security.pdf>)

Large-scale implementation of RFID into ports has not occurred yet. It is still in its early stages. Many trials and tests have been conducted at ports throughout the world. Benefits ranging from lower operating cost to higher efficiency of flow of goods have been experienced. RFID is able to provide reliable information at any time and be able to perform security tasks that would otherwise require many people and much time. An investment in RFID can, thus, serve two purposes: as a business accelerator in terms of supply chain efficiency, and as an enabler for improved security12.

#### RFID can resolve problems. Examples from the two largest supply chains prove

Hanebeck and Lunani 04-n.d.-08 (Chris Hanebeck and Mahesh Lunani, Lead RFID Consultant and Automotive Strategy and Change Practice Leader (respectively), “RFID-Enabled Returnable

Container Management”, IBM Global Business Services, <http://www-05.ibm.com/de/automotive/downloads/rfid-container-management.pdf>)

Most recently, RFID has been discussed in the light of Wal-Mart and the U.S. Department of Defense (DOD), the two largest supply chains in the world, who have mandated their suppliers to use the technology on all inbound shipments. RFID tags are attached to items, cases and pallets, and, when the items arrive at a loading dock, the tags can be read automatically alleviating the need for a manual, labor-intensive reconciliation. However, that is not the primary reason why the two organizations have invested in this technology. The true value lies in the visibility that RFID provides — seeing inventory whether in motion or in stock at all times. They have installed readers at all major choke points and know exactly when and where an item was last seen. For Wal-Mart and the DOD, the technology ultimately enables more intelligent planning, inventory management and procurement.

#### Increases Security

#### RFID increases security and speeds up the process

Talbot ‘6 (David Talbot, Chief correspondent of MIT Technology Review, “Ports' Technology Failure, MIT Technology Review, <http://www.technologyreview.com/news/405397/ports-technology-failure/2/>)

The national debate over port ownership and cargo security often features this sobering statistic: only 5 percent of cargo containers arriving in the United States are inspected. But perhaps an even more disturbing statistic is that fewer than 1 percent of cargo containers -- Pentagon cargo excepted -- are tracked with simple radio-frequency identification (RFID) tags -- a technology that could help pinpoint where a container has been and whether someone has broken its seal in transit. Each RFID tag can store a unique ID number that is "read" by fixed or handheld electronic readers. Such tags can also store bits of information from attached sensors. They present an obvious and relatively cheap way to help address the cargo security question. But the industry and government have barely begun to adopt this existing technology, says Daniel Engels, an MIT mechanical engineer and former research director at MIT's Auto-ID Labs, a leading center of research on RFID technology. The problem isn't a technological one, Engels points out. Rather, the industry has been slow to recognize a business model, governments aren't forcing the industry's hand, and the global cargo industry has not been motivated to forge standards. Daniel Engels: Outside of the Department of Defense and a few pilot programs around the world, I would say there are virtually no general cargo containers being RFID tracked. It's all done manually. There are some shipments within cargo containers being tracked with RFID; pharmaceutical companies have put tags on their shipments to get a temperature history, so they know when a refrigerator lost power. But those are shipments within containers. For containers themselves, the shipping companies have been slow to make a business case, and their customers are not forcing them along. DE: Of course, security starts by inspecting cargo when containers are loaded. Once that's done, RFID has a great potential to provide real-time visibility and intrusion detection, as well as quality measures within containers. With RFID tags and integrated sensors I can know exactly where that container is. I can know that nobody has tampered with it. It can also speed customs processes on both ends, thereby reducing delays.

#### RFID increase port security and don’t hinder trade.

Tsilingiris et al, 2007 (P.S., Laboratory for Maritime Transport – National Technical University of Athens, Greece, H. N. Psaraftis Laboratory for Maritime Transport – National Technical University of Athens, Greece, D. V. Lyridis Laboratory for Maritime Transport – National Technical University of Athens, Greece “RFID-enabled Innovative Solutions Promote Container Security” www.­martrans.­org:­8093/­docs/­publ/­REFEREED CONFERE­NCES/­SSE07 tsilingiri­s et al 2007.­pdf)

RFID-enabled applications in the OCI appear to partly confront the issue that originated them, namely, container security. The success of the first attempts and trials along with the rosy trends of RFID beyond the maritime industry fuel our cautious optimism regarding the adoption of RFID in the OCI. Our understanding is that aalthough the industry was very skeptical of RFID in the beginning, they were encouraged by the fact that the trials proved to reduce cost and time and to increase security levels. It appears that the major ocean carriers and the big ports will be the leaders of RFID adoption with smaller players being the followers. In general, the feedback from the industry is positive.

#### A2: Tampering

#### RFIDs are immune to tampering, increase economic efficiency and are cheap

Benin, 4/13/2004 (Joseph, “Radio Frequency Identification (RFID) Tags & Their Implication to Container Security” International Security Seminar Sam Nunn Security Program)

Physical Security The enclosed cases of the seals make them more difficult to physically tamper. Furthermore, as they are not in view, they are less likely to be subjected to whimsical physical handling. Finally, most RFIDs have internal circuitry that will alert a reader of its poor health should it be opened or damaged. Programmability The ability of a user to store information on the tag itself allows for much greater depth of information flow and efficiency. Processes can be recorded or personnel can “sign” when they inspected the item. Above all, the tags can be reused many times over for economic savings. Flexibility [5] Another advantage of RFID is design flexibility. RFIDs can be manufactured in any number of shapes, sizes, forms, materials, and can even be integrated in a product itself, such as the fabric of a shirt. Cost The cost of RFID tags is as varied as the features they provide. In mass quantity, passive RFIDs with minimal data capacity can cost as little as five cents each. Active RFIDs with expansive capabilities and a sizeable amount of storage, small footprint, and prolonged battery life can cost over $500.00 each.

#### A2: Reader Collisions

#### We can fix that

Benin, 4/13/2004 (Joseph, “Radio Frequency Identification (RFID) Tags & Their Implication to Container Security” International Security Seminar Sam Nunn Security Program)

Means do exist to solve or at least mitigate reader collisions. One such solution is the judicious allocation of frequency to readers to provide maximum separation among adjacent readers while also minimizing the duplicative assignment of any specific frequency. Another solution to this problem is the implementation of schemes, such as Time Division Multiple Access (TDMA) which “interleaves communication times on the same frequency” [13]. Overall, experts generally believe that reader collision problems faced within the RFID field are “simpler” than the frequency assignment problems faced by cellular telephone companies. If this is in fact the case, then finding solutions as reader collision situations arise should be more than feasible.

#### A2: Spoofing

#### We are prepared for spoofing

Benin, 4/13/2004 (Joseph, “Radio Frequency Identification (RFID) Tags & Their Implication to Container Security” International Security Seminar Sam Nunn Security Program)

There are quite a few built-in safeguards that protect the integrity of RFIDs, especially of the active variety. Secure RFIDs rely upon encryption to authenticate the tag itself (by signing with the tag’s private key) as well as integrity (by using the server’s public key to encrypt the data message). Additionally, an interruption in service automatically triggers an alarm. This encryption also protects against outsiders spoofing the RFID as the true public key of the RFID would not decrypt the message of the spoofing RFID. Finally, sensors continue to evolve and are providing more detailed, sophisticated, and comprehensive pictures of the cargo in transit.

#### A2: No Uniform Standards

#### They have uniform standards now

IDENTEC Solutions Aug 2011 (“Perfected Technology to Manage an Imperfect World” http://cdn.identecsolutions.com/wp-content/uploads/2011/08/Perfected-Technology-to-Manage-an-Imperfect-World.pdf)

Active RFID is the style of RFID that has been around the longest. It has remained, until the 18000-7 standard, a world of conﬂicting proprietary approaches ranging from frequency choice to low level protocol nuts and bolts. Over the years the read ranges have climbed from a couple of meters to 100 meters, battery life has been extended to 5 years, costs have come down, sensor technology has been incorporated, yet interoperability was still missing. There was no inherent advantage for any one vendor to share its technology or to push for a common approach – the market was still very much about differentiation due to the hardware technology itself. ISO 18000-7:2008, adopted and initiated by the US DoD, based on their practical experiences with a proprietary approach, has led to this break through.

#### A2: Costs Too Much

#### RFID tags are feasible and prices will continue to decrease.

Tsai 12-7-07 (Louis Tsai, Part of the University of California, Mechanical and Aerospace Engineering Department, “Container Tracking with RFID and Port Security”, WINMEC, <http://www.winmec.ucla.edu/rfid/course/2007f/Container%20Tracking%20with%20RFID%20and%20Port%20Security.pdf>)

The necessary hardware for the design and application of this RFID kit include RFID tags, sensors, and readers. RFID tags will be attached to the door and sensors will be placed inside the containers. Choice of sensors and other items used in correspondence with the tag are at the discretion of the user depending on need. Equipping one container can cost a few hundred to thousands of dollars. Although cost may be of concern, a new generation of active tags has brought the cost down considerably, making it more feasible to tag the tens of thousands of containers in use8. Also, as the RIFD technology matures, cost will also likely come down. The following are some basic hardware chosen to meet the basic needs.

#### RFIDs reduce costs in the long run outweighs any short-term decrease

Narsoo et al. n.d.-n.d.-09 (J. Narsoo is a Lecturer at the University of Technology Mauritius, W. Muslun was a postgraduate student at the University of Technology Mauritius, M. S. Sunhaloo is a Senior Lecturer at the University of Technology Mauritius, “A Radio Frequency Identification (RFID) Container Tracking System for Port Louis Harbor: The Case of Mauritius”, IISIT, <http://iisit.org/Vol6/IISITv6p127-142Narsoo691.pdf>)

Everyday millions of containers circle the globe and 250,000,000 container movements are performed around the globe yearly through 220 ports. Approximately 2% of in-transit containers are physically inspected, while empty containers are rarely inspected. A serious container event could trigger a worldwide massive port shutdown. Government security officials recognize container shipments as one of the world’s greatest security threats which press for dramatic improvements in air and maritime security. Port Authorities are striving to increase efficiency through effective supply chain management, while focus is being placed on control, visibility and security. This paper is based mostly on the possible implementation of an RFID (Radio Frequency Identification) based container tracking system for Port Louis harbor. RFID will enable the identification of containers over long distances and in demanding environments such as the port area. This will help in real-time identification and tracking of containers, reaching new levels of traceability and control. Companies will know at any point in time, where their assets are and all movements at key locations will be recorded for eventual streamlining and optimizations. These will lead to a reduced capital costs and significant overall savings in the long run for Port Louis harbor. The implementation of this system however relies on a solid collaborative network to link the various stakeholders of Port Louis harbor, by taking into considerations the specificities of Mauritius which is strategically positioned in the Indian Ocean.

#### Solves Economy

#### Active RFIDs increase security and don’t hurt the economy

Benin, 4/13/2004 (Joseph, “Radio Frequency Identification (RFID) Tags & Their Implication to Container Security” International Security Seminar Sam Nunn Security Program)

The big-picture gains from RFIDs come from the two significant improvements within such a system: dramatic increase in both the detail of information and the degree of automation. The unique codes allow for boxes, pallets, and containers to be rapidly tracked while in shipment. The greatest gains come in the area of security. RFIDs allow for the tracking of shipments in real time in order to ensure that they are following the correct route. The augmentation of sensors expands the ability to monitor the movement of goods. This results in greater levels of control of the supply chain and increased amounts of accurate information. Ultimately all of this results in greater knowledge about the contents, condition, and continuity of what is being tracked, bringing about safer ports and greater profits.

#### Implementing RFID technologies improves economic output of trade. Its key to reduce costs and increase security.

Benin, 4/13/2004 (Joseph, “Radio Frequency Identification (RFID) Tags & Their Implication to Container Security” International Security Seminar Sam Nunn Security Program)

Small-scale gains in converting to RFID modes of operation are best seen in contrast to the use of barcodes. RFID technology allows for much greater throughput, which has direct monetary benefits. Additionally, the higher level of detail results in smarter inventory management. This provides a means of preventing “shrinkage” caused by “employee and customer theft, vendor fraud, and administrative error,” which accounts for a loss of nearly two percent of total sales [14]. Furthermore, a study by Gap clothing has found that having all the right sizes in the right place results in greater profits [15]. Thirdly, there is direct labor cost savings in the use of RFID tags. No time is needed to handle goods and scan them, while considerable labor costs are involved in a barcode system. It is estimated that RFID can decrease 25% of labor time used in inventory and sale transactions [15]. Thus the benefits of RFID at the micro-level can be summarized “in terms of labor savings, anti-diversion track-and-trace ability, and supply chain visibility” [15]. Beyond these efficiency savings, there are a number of external factors outlined in “Web-Based RFID: Hype or Glimpse of the Future?” that will serve as a catalyst in the adoption of RFID among retailers. The first deals directly with container security: the Customs and Border Patrol’s Container Security Initiative. This push to digitize the trade documentation coupled with the 24-hour rule is placing increasing pressure to provide accurate manifests that are acquired in the most non-labor intensive method possible. RFIDs meet these needs. Secondly, on January 1, 2005, an additional digit will be added to barcodes, requiring the barcode infrastructure to upgrade. It is quite plausible that between now and then businesses will choose to either replace their barcode systems with RFID ones or install dual-functionality consoles. The third factor creating an environment conducive to RFID adoption at the unit level is the recently announced Electronic Supply Chain Manifest (ESCM) that will place the same documentation requirements on domestic trade as that of international. Its implementation is set for the 2005-2006 time frame [15]. The final factor is that of Wal-Mart’s RFID Strategy. Wal-Mart is requiring that its top 100 suppliers must begin using RFID chips at least at the pallet level by January 2005. It is estimated that if the “top 100 suppliers to the top 30 retailers” started using RFID, almost 80% of all consumer goods would be tagged!

#### RFIDs Are Transportation Infrastructure

#### RFIDs are transportation infrastructure.

Qiao et al, June 2009 (Fengxiang, Lei Yu, Rong Zhang, Zhiyuan Chen, Reza Fatholahzadeh “RFID Applications in Transportation Operation and Intelligent Transportation Systems (ITS)” Research Report Center for Transportation Training and Research Texas Southern University http://swutc.tamu.edu/publications/technicalreports/476660-00044-1.pdf)

Radio frequency identification (RFID) transmits the identity of an object or a person wirelessly. It is grouped under the broad category of automatic identification technologies with corresponding standards and established protocols. RFID is suitable for applications in different industries and has penetrated into several aspects of our lives. The versatile features and benefits of RFID technology have proven that RFID can be widely applied in the field of transportation to improve driving safety, reduce vehicle collisions, and even help reduce vehicle emissions. Generally speaking, the applications of RFID in transportation are still limited and are not scanned and summarized well. This paper aims to conduct an extensive literature review to identify the existing and potential applications of RFID and its research opportunities and needs in transportation. Existing applications in transportation fields have been identified such as safety, operation - including Intelligent Transportation System (ITS) and Vehicle Infrastructure Integration (VII), security, policy, etc. Obstacles that possibly frustrate the wide and in-depth applications of RFID in the transportation area are in the aspects of technology, cost, policy, and privacy. RFID is one of the most forceful technologies that will affect a variety of aspects in transportation including ITS. It is believed that RFID-based technologies can be extensively exploited to improve transportation safety and security, increase the efficiency of the transportation system, ultimately save costs, and, therefore, improve the quality of human lives.