American Enterprise Institute for Public Policy Research

Is Port Security Spending Making Us Safer?

Veronique de Rugy
American Enterprise Institute

AEI WORKING PAPER #115, SEPTEMBER 7, 2005

www.aei.org/workingpapers
www.aei.org/publication23138
18935

Outline

I. Introduction

II. The Economic of Port Security Spending
- II.1. Direct Threats to Ports
  - II.1.a. How should ports be protected?
  - II.1.b. Which ports should be protected?
  - II.1.c. Who should do the protection?
- II.2. Transportation of WMD through Ports
  - II.2.a. How should ports be protected?
  - II.2.b. Which ports should be protected?
  - II.2.c. Who should do the protection?
- II.3. Conclusion

III. Port Security Spending
- III.1.How are we spending the money?
  - III.1.a. The Port Security Grant Program
  - III.1.b. Transportation of WMD through Ports
- III.2. Is DHS achieving its objectives?
  - III.2.a. The Port Security Grant Program
  - III.2.b. Transportation of WMD through Ports
- III.3. Should DHS be prioritizing different objectives for port security?
  - III.3.a. The Port Security Grant Program
  - III.3.b. Transportation of WMD through Ports
- III.4. Prioritizing port security within homeland security

IV. Conclusion

I. Introduction

Congress should direct homeland security funding to programs that provide the greatest return in the most crucial security missions. Since the number of possible attacks is effectively unlimited and the resources we can devote to the fight against terror are limited, spending should not occur without a careful cost-benefit analysis. Most importantly, it is perfectly reasonable to decide not to implement an antiterrorism measure, not because it has no benefit, but because the costs are too high compared to the potential benefits. Of course, programs that are not cost effective should never be implemented.

The greatest threats should be addressed first. The Department of Homeland Security (DHS) should prioritize threats that have a relatively high probability of occurring and pose catastrophic consequences. It should then develop, acquire, and set in place the tools and techniques needed to prevent, respond, or recover from such awful scenarios. By this rubric, nowhere is it more important to develop cost-effective security plans than in the area of maritime security.

According to experts, the U.S. should be concerned about nuclear attack by sea. More than 85 non-proliferation and national-security experts polled for a congressional study estimate that the risk of a WMD attack in the next decade using some sort of nuclear device is as high as 70 percent.[1] And Stephen Flynn, a Senior Fellow in National Security Studies at the Council on Foreign Relations, reported that the CIA has concluded that the most likely way weapons of mass destruction (WMD) would enter the United States is by sea.[2]

This is a serious threat: the Council on Foreign Relations estimates that a less-than-perfect one kiloton nuclear bomb in lower Manhattan would immediately claim 200,000 lives, injure 200,000 more and may kill half the population exposed to radiation few weeks later.[3] A rough estimate shows that the direct economic cost of such a tragedy would run over $1.1 trillion (see table 1).

There is little doubt that our ports offer terrorists vast opportunities to inflict terrible damages on our country. The U.S. maritime system includes more than 360 sea and river ports with more than 3,700 cargo and passenger terminals and more than 1,000 harbor channels along thousands of miles of coastline.[4] Maritime shippers have increasingly concentrated their traffic through major cargo hubs (called megaports) because of their superior infrastructure. Approximately 85 percent of all cargo tonnage exchanged in the United States passes though just 50 seaports scattered throughout the country.[5]

In addition, maritime commerce is essential to America's economic vitality. As the primary mode of transportation for world trade goods, ships carry more than 95 percent of the nation's non-North-American trade by weight and 75 percent by value, and 100 percent of the foreign oil imported by the United States.[6] In 2003, waterborne trade contributed about 7.5 percent of the U.S. gross domestic product.[7] Given the importance of maritime trade to the U.S. economy, disruption of that trade would have immediate and significant economic consequences in the United States and also worldwide.[8]

Considering the scope of maritime opportunities for terrorists and the dramatic consequences of a successful nuclear or radioactive attack nowhere is the need for strategic spending more apparent than in the area of maritime security.

In FY2006, President Bush requested a budget of $2.03 billion for port security out of a $50 billion budget for homeland security activities government wide. However, on homeland security issue, the important question is not how much money is spent but rather whether the money is allocated toward the most cost-effective programs. In other words, is America getting the maximum level of benefit in exchange for the spending?

This paper reviews some homeland security port programs. First, it takes a look at the economics of port security spending. Second, it examines how the federal government, mainly through DHS, responds to the two main terrorist threats faced by ports: (1) direct threats on the ports themselves and (2) indirect threats via the transport of dangerous material through ports for use in terrorist plots elsewhere in the country. Third, it analyzes whether DHS is achieving its port security objectives and then whether this spending is conducive to improving port security and security in the United States. Finally, this paper will look whether this allocation demonstrates good prioritizing within homeland security

This paper will show that port security spending appears to occur without risk and cost-benefit analysis, leading to large array of misallocated of spending. For instance, a close look reveals that within port security spending per se possibly less money is appropriated to the highest priorities such as preventing nuclear devices from blowing up in our ports than to nuclear detection on site (when it would already be too late). Also, much of the appropriated money is allocated to ineffective programs or low priority goals such as the Port Security Grant Program or Radiation Portal Monitors. But this prioritizing seems also to be lacking within Department of Homeland Security's budget.

Allocating money efficiently means that the money appropriated must be spent based on risk analysis. To be most effective, the money should first go to programs preventing devastating terrorist attacks, i.e., intelligence programs. And if experts are correct about the probability of a nuclear attack in our country then the federal government should make protection of stockpiles of fissile materials a priority. Within maritime security, funds should also fund the highest priorities first, like keeping nuclear weapons and terrorists outside of our ports.

Finally, if funds are spent on ports to upgrade security then the money should go first and foremost to critical national ports and terminals—the areas of highest consequence with the greatest vulnerability to terrorist attack—rather than spending a little money in every port. Severely damaging one of these critical ports could not only cause injuries, death, and property damage, but could also disrupt the flow of basic goods into and out of the country. Spending a little money everywhere ensures that we protect nowhere adequately.

II. The Economics of Port Security

In the war on terror, the federal government has identified thirteen critical sectors that the country needs to protect from terrorism including agriculture, banking, government, public health, and transportation. Each sector is competing for limited anti-terrorism dollars.

Economists think about security policies in terms of tradeoffs, formally comparing the costs and the benefits, both pecuniary and non pecuniary. In other words, homeland security funds should be allocated among sectors based on the probability of something happening, the likelihood of it succeeding, and the consequences of it occurring and using policies that would provide the biggest return on taxpayer's dollars. This regime should be maintained throughout the allocation process and should dictate how funds are dispersed within each sector.

When we apply this structure to spending aimed at combating terrorist threats to U.S. ports, we must recognize that there are two types of threats related to ports: (1) direct attacks on the ports themselves and (2) transport of dangerous material through ports for use in terrorist plots elsewhere in the country. By far the most important task is protecting against admission of dangerous materials, since the damage from fissile materials would likely be on the order of 100 times greater than any damage to a port could be.

We should be leaving direct port protection to local port authorities and the private sector. For reducing the risk of admission of dangerous materials, we should focus spending on intelligence and physically protecting stockpiles of fissile materials.

II. 1. Direct threats to ports

As detailed above, our extensive maritime system offers terrorists many opportunities for attack. Like any terrorist attack, an attack on a port could cause injury and death, but because of the vital role of maritime commerce in the American economy, it would also have terrible economic consequences. Damage to infrastructure and the destruction of inventory in port could seriously disrupt trade not only in the U.S., but also around the world.

II.1.a. How should ports be protected?

In ports, as with all stationary targets, the attacker has a natural advantage because he gets to choose where to attack. The German thrust into Western Europe in World War II is a natural analog: The Wehrmacht simply side-stepped the impressive defenses built by the French in the Maginot Line. Similarly, terrorists will attack wherever the defenses are weakest.

Because of this advantage for terrorists, intelligence gathering and counter-intelligence are often the most cost-effective defense. The defender can thwart the attackers before the attack is even launched or deploy personnel and equipment exactly where the attack is anticipated.

The second-best solution is to mitigate damage after an attack. Without knowing where or how the attack will occur, the defender can lower the expected damage by developing plans for the aftermath of an attack. For a port, such plans might include evacuating civilians and personnel, placing emergency equipment within easy reach,

training personnel to handle emergencies and attacks, and developing business continuity strategies to allow the port to get up and running quickly after an attack.

The third-best option for defending against direct attack is direct prevention. Such defenses include physical barriers (e.g., fences), surveillance equipment (e.g., closed-circuit television), and access control systems for employees and visitors. Given that such direct defenses are only as good as their weakest link, they tend not to be cost effective: one has to protect *everything* from *every* possible mode of attack.

So, as with almost all counter-terrorism, the focus should be on intelligence. But if intelligence is not possible or adequate, the focus should be on damage mitigation. Direct prevention should be only the last resort.

II.1.b. Which ports should be protected?

The objective of counter-terrorism is to minimize expected damage. Expected damage equals the probability of attack times the damage if attacked. Because terrorists will tend to focus on targets with the greatest potential for damage, the ports facing the greatest probability of attack and the ports where attacks would be most damaging are one and the same. All else equal, these ports are the largest ones, where an attack would stop a significant amount of trade and have a considerable economic impact.

According to Stephen Flynn, a Senior Fellow in National Security Studies at the Council on Foreign Relations, the twin ports of Los Angeles and Long Beach are by far our most vulnerable target. The two ports handle over 40 percent of the total container traffic flowing in and out of the United States. If a terrorist attack shut down that traffic, it would have an immediate spillover effect, causing gridlock in Hong Kong, Singapore, Rotterdam, and every other major trading port reliant on the world's biggest economy.

Key U.S. imports, starting with oil, would become scarce almost immediately. Factories would become idle for lack of raw materials or spare parts. Places like Hawaii, which depend on shipping for almost every consumer need, would quickly run out of food.

According to 2003 data from the American Association of Port Authorities, the total trade disruption cost of a daily shutdown of the twin California ports would be roughly $600 million.[9] The daily cost of the total shutdown of the megaport of New York/New Jersey would be $277 million.[10] By contrast, the shutdown of a small port like Richmond, Virginia would yield a daily cost of $3 million.[11] That number does not take under consideration the cost to the economy as a whole. The megaport of New Orleans for instance yields roughly 20 percent of the annual U.S. GDP. It devastation and shutdown following the hurricane Katrina at the end of August 2005 will yield dramatic economic loss for our economy.

In addition to the larger economic effect from attacking a large port, the death toll is also likely to be higher in a megaport because of the greater passenger traffic and the many people working on site.

Some characteristics of large ports make protection costs per ton of cargo higher than in smaller ones. For instance, the larger number of people around megaports probably also makes it easier for terrorists to blend in undetected, which increases the probability that an attack is successful. Also, megaports are extremely complex and dynamic, making it difficult to determine a comprehensive security picture.

On the other hand, some other characteristics of larger ports make protection costs per ton of cargo lower than in smaller ports. First, the perimeter of a large port is proportionally smaller than for a small port. Second, security systems have high fixed costs but low marginal costs; that is, access-control systems, for instance, do not cost much more when there are more employees. Third, there are economies of scale in security processes (e.g., a large-enough staff to cover breaks, greater experience of the staff, from greater exposure).

But even if protection costs in larger ports were lower than in smaller ones, protection for megaports would still be more cost effective. We should allocate relatively more money, or even all money, to larger ports because the consequences of an attack there would be significantly larger and because their visibility and the high volume of cargo exchanged make them subject to a greater probability of attack. In short, the expected damage is greatest at the largest ports, so they should be the focus of our counter-terrorism efforts.

II.1.c. Who should do the protection?

Protection through intelligence is a public good, which means that one person's consumption of the good does not prevent another person from consuming the same good.[12] Another characteristic of public goods is that they are non-excludable, i.e., it is hard or impossible to prevent anybody from getting access to and enjoying the public good once it is produced. Economic theory suggests that it is efficient to have governments provide public goods, but to resort to private markets for the provision of non-public goods.

In the case of intelligence-gathering, the insights we gain could apply to any port. It would not be cost effective for each port operator to try to infiltrate terrorist networks to discern whether that given port was to be attacked. Given this public-good nature of intelligence, such activities should be funded by the federal government.

But the current thrust of federal spending on port protection is on direct prevention via physical barriers, direct surveillance, and access control. None of these prevention techniques is a public good: the cost to the port is the same as the cost to the government. And as with other government spending, a local or private decision-maker is in a better position to determine local needs and the most effective way to meet them. As a result, all such spending should be local, e.g., paid for from taxes and fees charged by the port in question.

The most cost effective use of our federal dollars is to keep bad things from happening inside our ports by stopping terrorists before they attack. However, assuming that not every attack can be prevented, some level of direct defense is wise. But if we are going to invest money to protect ports directly, the most cost effective measure is to protect the megaports. And it should be done without subsidy from general tax revenue.

II. 2. Transportation of WMD through ports

The second type of terrorist threat related to ports is the transport of dangerous material through ports for use elsewhere in the country or in the ports themselves. If those materials are used to build weapons of mass destruction, either nuclear or radiological, the damage is likely to be orders of magnitude more severe than from a direct attack on a port.

Unfortunately, this serious threat is not as unlikely as one would like it to be. National security experts have estimated that the risk of a WMD attack in the next decade to be as high as 70 percent.[13] WMD attacks figured in two-thirds of the 15 disaster scenarios the U.S. Homeland Security Department identified last year and uses to measure our level of preparedness.

To be sure, the technical expertise to make and use a nuclear weapon is considerable. However, according to Charles D. Ferguson, a science and technology fellow at the Council on Foreign Relations, and William C. Potter, the director of the Monterey Institute's Center for Nonproliferation Studies, (2004), the real nuclear threat comes from terrorists obtaining the key ingredient of a nuclear bomb and then producing a less-than-perfect, but usable, nuclear device delivered by something as common as an ocean freighter.[14] That, they think, could be achieved just a few years down the road.

In the short term, the most likely threat arises from radiological materials packed with conventional explosives to create a so-called dirty bomb. In addition to the damage created by a regular bomb, a dirty bomb spreads radioactive materials in the air. According to the Central Intelligence Agency (CIA), the Al Qaeda terror network is fully capable of building a radioactive “dirty bomb” targeting the United States and other Western nations and “has crude procedures” for producing chemical weapons.[15] More troublesome are allegations of Al Qaeda’s interest in acquiring fully developed nuclear capabilities.[16]

The probability of a terrorist attack with an actual nuclear weapon cannot be reliably estimated, and it is surely lower than the probability of virtually any other type of terrorist attack. But the devastation from such an attack would be so overwhelming that, based on expected damages—the probability multiplied by the consequences—this threat must be considered one of the greatest dangers America faces.

According to the Council of Foreign Relations (CFR), the blast from a one-kiloton nuclear weapon—such as a crude improvised weapon or a stolen battlefield weapon—in midtown Manhattan during the day would kill more than 200,000 people and injure at least 200,000 more. It would also produce radioactive fallout that could kill half the exposed population as far as three miles away within a few weeks. And it would destroy most buildings and other structures over 11 city blocks as well as seriously disrupt Manhattan’s transportation, communications, utilities, and other infrastructure.[17]

Based on the CFR’s assumptions, Table 1 shows an imperfect estimate of the direct cost of a successful terrorist attack using a one-kiloton nuclear weapon in selected U.S. cities: lower Manhattan, downtown Chicago, downtown Washington DC and downtown Los Angeles. To put this blast yield in perspective, a one-kiloton device has less then 10 percent the yield of the 1945 era “little man” weapon used in the bombing of Hiroshima.

Table 1. Estimated cost of the blast from a one-kiloton nuclear weapon in selected U.S. cities

Cities	Total ($million)
Lower Mahattan	$1,153,766
Downtown Chicago	$217,026
Downtown Washington DC	$158,092
Downtown Los Angeles	$134,019

Note: These costs do not include the lost of economic output or the cost of cleaning up the contamination from the radioactive fallout. These costs would add at least several hundred billions to the total.

Source: Council on Foreign Relations (2005), "Terrorism: Questions & Answers, Responding to Nuclear Attacks;" Aldy and Viscusi (2003), "Age Variations in Workers' Value of Statistical Life," NBER Working Paper No. 10199; Area and Population Density from 2000 County and City Data Book; Office space from CB Richard Ellis Real Estate;NYC Comptroller's estimate of 9/11construction cost from per sq. ft.

Using 2000 population density numbers, we can deduce that if such a device were to kill 200,000 people and destroy 11 city blocks in Manhattan, 38,160 people would be killed in Chicago, 27,880 in Washington D.C., and 23,570 in Los Angeles.[18]

According to Aldy and Viscusi (2003), the value of statistical life for 30 to 40-year olds is at least $5 million in 1996 dollars.[19] This number is consistent with Viscusi's review of the literature (1993), which finds that most studies estimate the value of life to be between $3 million and $7 million in 1990 dollars.[20] Using the estimate of $5 million in 1996 dollars, the value of life is $5.766 million in 2004 dollars. We therefore estimate the cost of 200,000 lives lost to be $1.1 trillion, the cost of 38,160 to be $217 billion, the cost of 27,880 to be $158 billion, and the cost of 23,570 to be $134 billion.

We can also estimate the cost associated with the destruction of 11 city blocks in each of the selected cities. If we assume that the length of 11 blocks equals 1 mile then the area of 11 blocks is about 0.1 square mile. Assuming that most of the buildings destroyed downtown in big cities would be office buildings, we find the average office space per square mile in each city. After September 11, most experts used the New York City Comptroller's construction costs estimate to measure the cost of a terrorist attack leading to building destruction. This construction cost is roughly $500 per square feet,[21] which means that the construction cost for 11 city blocks would be $765 million in New York, $26.1 million in Chicago, $91.6 million in Washington D.C., and $18.1 million in Los Angeles.

To conclude, a crude estimate of the direct cost of immediate deaths and destruction of 11 city blocks due to the use of a one-kiloton nuclear weapon would be $1.1 trillion in New York City, $217 billion in Chicago, $158 billion in Washington D.C., and $134 billion in Los Angeles. Of course, this number is a gross underestimate of the total cost—though the order of magnitude is correct—since it does not consider indirect costs from cleanup, economic disruption, and injuries after the explosion, or treatment for all the people exposed to radiation during the attack whom would develop serious diseases several years down the road. [22] These costs would be huge.

According to the Nuclear Threat Initiative experts, the costs related to the disruption of economic activities, such as the loss of economic output in the city attacked,

would likely total several times the direct cost amount.[23] The New York City Comptroller estimated that the weekly output of lower Manhattan was $2.1 billion per week, while that of the rest of the city combined was $6.3 billion per week.[24] In the wake of a blast such as that envisioned, a conservative estimate claims that the output of lower Manhattan would be reduced to zero for two weeks and permanently reduced by one third.[25]

That means a loss of over $50 billion per year. To these figures must be added the immense cost of cleaning up the contamination from the radioactive fallout, which would run into the tens of billions of dollars. In short, several hundred billion dollars should be added to the direct cost reported in Table 1.

More likely than a nuclear attack is the use of a dirty bomb. U.S. and British intelligence have reportedly concluded that Al Qaeda has succeeded in making such a bomb.[26] Fortunately, even though the probability of a dirty bomb is much higher than the probability of a nuclear attack, such a weapon is a far cry from an actual nuclear explosive. Of all weapon of mass destruction (WMD) attacks, a dirty bomb attack is unlikely to cause mass casualties on the order of a nuclear bomb and few, if any, casualties would immediately result from radiation exposure.[27] Yet, a dirty bomb device detonating in New York City would still result in massive costs.

The biggest cost of a dirty bomb attack would be the required cleanup. Zimmerman and Loeb (2004) estimate that the consequences of a dirty bomb attack on lower Manhattan might exceed the costs to restore New York City after the September 11 attacks.[28] The New York City Comptroller estimated the economic cost of 9/11 at roughly $94.8 billion.[29] In other words, even the least devastating WMD attack in New York City using a dirty bomb would end up costing at least $95 billion in damage.

Table 2 recapitulates the estimated cost of three different terrorist attack scenarios on New York City and its port.

Table 2. Estimated cost of three terrorist attack scenarios in New York City

Scenarios	Estimated costs
One-kiloton nuclear bomb in NYC	$1.1 trillion
Dirty bomb in NYC	$95 billion
Non nuclear attack on NYC port ceasing operation for a month	$10 billion

Note: These number are low estimates but order of magnitude correct.

Source: Table 1 and Peter D. Zimmerman and Cheryl Loeb (2004), "Dirty Bomb: The Threat Revisited," Defense Horizons, the Center for Technology And National Security Policy At National Defense University, Number 38; Port Authority of NY and NJ Annual Data.

The cost of an attack on NYC port is based on a daily cost of $277 million to shutdown of the megaport of New York/New. Although imperfect, these estimates nevertheless help give us an idea of the consequences of the three types of attacks. Considering the devastating costs of attack, nuclear or radiological terrorism is the one threat that requires zero tolerance. Preventing a nuclear or a dirty bomb from going off in the United States is a public good and should be the role of the federal government. Moreover, it should probably be the federal government's top priority.

II.2.a. How should ports be protected?

Expert Stephen Flynn reports that "the CIA has concluded that the most likely way weapons of mass destruction (WMD) would enter the United States is by sea."[30] The odds are high that if terrorists bring nuclear devices into the U.S., it will be through a port. For that reason, we must secure our ports to stop the transportation of nuclear devices into the United States. However, to get the biggest return on our security investment, the threat needs to be addressed in a cost effective manner.

The secrets of nuclear weapon design were revealed long ago. Today, the only significant barrier to building a weapon of mass destruction remains access to fissile (highly enriched uranium and plutonium) and radiological materials. Terrorists have two options. They could either acquire a complete, ready-to-use weapon or they could acquire the materials and components to build the weapon themselves. While the first scenario cannot be ruled out, the second scenario is more likely. According to Captain Joseph Bouchard, a retired Navy Officer and an expert on nuclear devices, nuclear and radioactive material is considerably more difficult to acquire in the United States than overseas.[31] The rest of the materials required to assemble a bomb, however, could be acquired in the U.S. Consequently, the most likely scenario is that terrorists would get dangerous fissile materials abroad, smuggle them into the U.S., and then assemble the bomb here.

Law enforcement agencies face an enormous challenge in protecting the country's borders from smuggling, whether it is drugs, illegal immigrants, stolen goods, or dangerous materials like uranium. 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, the probability of stopping terrorists from smuggling something into the country is very low.

Drug smuggling is a good case in point of how easy it is to smuggle illegal goods into the U.S. According to Barry R. McCaffrey, the former director of the Office of National Drug Control Policy, virtually all cocaine and heroin, and a majority of marijuana, sold and consumed in this country is produced abroad and then smuggled into the country.[32] In 2000, the total amount of cocaine and heroin consumed in the United States was 259 metric tons.[33] This is roughly equivalent to 300 pickup trucks full of drugs.

Contrast that number with the information from the U.S. Department of Justice that, in 2002, the Drug Enforcement Administration seized 59.1 metric tons of cocaine and heroin: the amount of smuggled drugs dwarfs the amount of captured drugs Clearly, determined smugglers have no difficulties passing through porous U.S. borders.

Considering the extreme difficulty of interdicting drug smugglers, it seems that determined smugglers with a nuclear device would have little trouble circumventing the nation's border protection and control, particularly because they would be able to leverage the techniques used successfully by drug smugglers. Further lowering their probability of being caught is the fact that, according to a series of experts testifying

before Congress in July 2005, terrorists could easily shield the highly enriched uranium and avoid detection from radiation detectors.[34]

Considering these factors, to prevent a nuclear device from entering the country, the first best solution will always be to make sure that terrorists do not get the dangerous materials necessary to build a bomb. The most cost effective solution would be to keep close tabs on fissile materials. It is easier to monitor a lump of uranium at a known location than to detect uranium smuggling. Part of this exercise might include buying foreign stockpiles or helping foreign governments protect or destroy their stockpiles. This approach could be summed up in five words: "no fissile material, no bomb."

The second best solution is to invest in intelligence about future attacks or about who is seeking or has obtained fissile materials. According to Laura Holgate, an expert at the Nuclear Threat Initiative, while it is relatively easy to get intelligence about the supply of fissile materials, it is much more difficult to acquire intelligence of the demand for these products.

If terrorists were ever to obtain fissile materials, they would have two options. One, they could either smuggle the material into the U.S. to blow up a city. Two, they might consider the low probability of getting caught at the border too high to risk it and thus decide to blow up their bomb while entering the port rather than inside the country. Even though the damages would be less than the damages caused by a bomb inside New York City, an attack in the port would still be catastrophic.

The third best solution is to put in place security mechanisms to prevent nuclear devices from arriving in the United States. For instance, we should help officials abroad to tighten security at the foreign ports that feed shipments to the U.S. These efforts could include helping fund systems to bolster foreign countries' ability to detect nuclear material in their ports or placing U.S. agents on site in foreign ports.

To prevent dangerous material from entering U.S. ports, another cost effective strategy would be to create partnerships with foreign manufacturers and importers. Partners would agree to meet "supply chain" standards establishing a secure chain of custody for every unit of cargo traded overseas. This would ensure that their shipment methods repel potential terrorist attempts to use those shipments for introducing weapons of mass destruction into our ports. These partnerships would reduce the need of screening every cargo equally.

Finally, the fourth best solution is direct onsite detection at local ports. This is the least cost effective measure because, according to experts, it is hard to detect highly enriched uranium and almost impossible to detect anything if it is shielded. As such, the effectiveness of the detection devices we have now is dubious. However, even if the detection devices were capable of detecting dangerous material, it would still be riskier than the three other solutions because the stakes are so high: if the system fails, the illicit material ends up inside the country.

II.2.b. Which ports should be protected?

Unlike direct threats to ports, where larger ports present more attractive targets for terrorists, when it comes to transporting WMD material through a port, terrorists are agnostic: they will exploit whichever port has the most porous security. Spending to thwart admission of WMD materials should therefore seek to make all ports equally secure. Roughly speaking, this will mean that each port's counter-WMD spending

should be roughly proportional to its volume. For example, if gamma-ray detectors are used in one port, then they should be used in all ports. Providing these detectors would cost the same per ton of cargo in all ports, so a port with twice the cargo volume would require twice the number of detectors and twice the budget for counter-WMD expenditures.

II.2.c. Who should do the protection?

Like intelligence gathering, preventing a nuclear or radiological bomb from going off in the United States is a public good. Espionage, intelligence, and nuclear threat reduction benefit all the states, so the *federal* government should make these investments.

National security experts estimate that the risk of a WMD attack in the next decade using some sort of nuclear device is extremely high.[35] If they are correct, then preventing terrorists from getting their hands on WMD should probably be the federal government's top priority.

The threat of WMD materials entering through ports is much more serious than direct threats to ports. The best ways to protect against WMD are, in descending order: (1) control stockpiles of fissile material, (2) gather intelligence on planned attacks, (3) prevent dangerous material from being loaded into a U.S.-bound cargo vessels, and (4) detect WMD material upon entry into a U.S. port. All four of these preventive techniques have public-good aspects, so economic theory tells us that they should be the responsibility of the federal government.

II. 3. Conclusion

There are two types of terrorism threats related to ports: (1) direct threats to the ports themselves and (2) transport of dangerous material through ports, for use in terrorist plots elsewhere in the country. If experts are correct about the high probability of a terrorist WMD attack, then the most important task by far is to protect against admission of WMD materials, since the damage from fissile materials would likely be on the order of 100 times greater than any damage to a port could be.

We should be leaving direct port protection to local port authorities and the private sector. For reducing risk of admission of dangerous materials, we should focus spending on intelligence and physically protecting stockpiles of fissile materials. Figure 1 summarizes our findings about the economics of port security spending.

Figure 1: Chart of Cost Effective Port Security Spending

	Direct Threats to Ports	**Transportation of Dangerous Material through Ports for Use into the US**
Federal	1. Intelligence to thwart attacks before they are launched	1. Intelligence and Protection of fissile material stockpiles 2. Security mechanisms abroad to keep WMD out of our port 3. Direct WMD detection on site at local ports
State and Local	1. Mitigate damage after an attack (i.e., emergency equipment, business continuity practice) 2. Upgrade security in ports (physical and operat	N/A

III. Port Security Spending

The attacks of September 11, 2001 renewed lawmakers' focus on protecting the country's port facilities. As a result, in FY2006, the President has requested $2.03 billion to fund port security. The U.S. Coast Guard (USCG) and Customs and Border Protection (CBP) are the federal agencies with the greatest involvement in seaports and most of the spending occurs through them, but other agencies, such as the Transportation Security Administration, are also involved.[36]

The spending total includes the Port Security Grant Program, the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, and the Weapon of Mass Destruction Detection Technology Programs, a portion of the Coast Guard's $1.5 billion homeland security operating expenses for ports, and the FY2005 share of the Coast Guard acquisition and modernization program.[37]

The Port Security Grant Program is the only major direct grant program for ports. Its purpose is to improve physical and operational security. Congress allocated $150 million out of which $140.4 will be distributed in September 2005. But the program has received over $706 million through FY2005.[38]

Part of the port security funds will also be spent to protect the U.S. against the admission of WMD materials for use inside the country. In FY2006, an estimated $500 million will be spent on that mission in ports at home and abroad. Parallel to DHS's efforts, the federal government—mainly through the Department of Defense and the Department of Energy—will spend an estimated $1.2 billion on nuclear threat reduction.

The $150 million grant program represents 0.3 percent of the $50 billion budget for homeland security related activities in FY2005 budget.[39] Overall, port security spending represents 4.2 percent of total homeland security spending, which is a small amount compared to the $4.7 billion—9.4 percent—directed to airport security.[40] It is also less than what DHS spends on first responder grants to state and local governments.

In this section, we will look at port security spending in two categories—spending meant to address direct threats to ports and spending meant to address the transport of dangerous material through ports for use into the U.S . We will first explain how the money is spent, then whether this spending is aligned with DHS's objectives. We will then measure the spending against the objectives identified in Section II to determine whether this money is used in a cost effective manner.

III. 1. How are we spending the money?

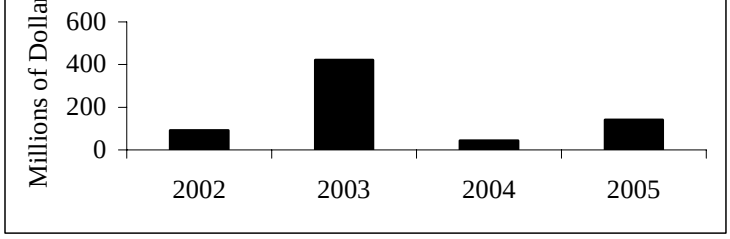
III.1. a. The Port Security Grant Program

The Port Security Grant Program (PSGP) has a narrow focus. It concentrates on funding security upgrades such as new patrol boats, surveillance equipment at roads and bridges, and new command and control facilities, in the hope of mitigating direct attacks on ports. In 2002, Congress provided the first wave of funding to the Transportation Security Administration (TSA), then part of the Department of Transportation, to enhance the security of ports and other facilities. TSA, along with the Maritime Administration (MARAD) and the U.S. Coast Guard (USCG), developed the PSGP, which it continued once it became part of the Department of Homeland Security. In May 2004, the PSGP was transferred to the Office of Domestic Preparedness (ODP).

The grants are awarded to state and local governments and private companies. Eligible applicants in each port area may submit one application for funding. Each applicant that meets the requirements of the PSGP Guidelines and Application Kit is evaluated by a field review panel and a national review panel. Grant recipients are selected through a competitive process.

Figure 2 shows the trend in PSGP expenditures since 2002. In FY2002, the TSA received a total budget of $1.24 billion, of which $92 million was dedicated to the new Port Security Grant Program.[41] Since this first round of awards, DHS has funded more than 1,300 port security projects over three years: PSGP allocated $170 million in July 2003, $179 million in December 2003, $49 million in September 2004, and $140.9 million in May 2005, [42] and the Urban Area Security Initiative provided $75 million in August 2003.[43]

Figure 2: Trend in the Port Security Grant Program Between 2002 and 2005



Source: Department of Homeland Security, Office of Domestic Prepardness FY2002, FY2003, FY2004 and FY2005

The total amount allocated to port security grants over four years is $706 million. In addition, the Transit Grant Program for ferry security received an additional $5 million in FY2005.[44]

Interestingly, the Port Security Grant Program represents a small portion of port security money—les than a percent—and is only 0.3 percent of homeland security spending government wide. Yet, each year, the House and the Senate fight over the amount this program will receive. This year was no exception. In other words, the Port Security Grant Programs is a very political program because it is a very visible program that Congressmen like to use to show their commitment to homeland security and to their constituents.

III.1. b. Counter-WMD activities

According to the September 11 Commission, “the greatest danger of another catastrophic attack in the United States will materialize if the world’s most dangerous terrorists acquire the world’s most dangerous weapons.”

The odds are high that if terrorists bring nuclear devices into the U.S., it will be through a port. According to Bethann Rooney (2005), the Manager of Port Security at the Port Authority of New York and New Jersey, likely threat scenarios include the use of vessels and ports as a means to smuggle weapons of mass destruction or terrorist operatives into the United States, the use of ships as weapons, the scuttling of ships in

major shipping channels, and attacks on ships such as ferries or oil tankers.[45] She explains that, "Since 9/11, we have seen a number of these tactics used around the globe in events such as suicide bombings using containers in the Port of Ashdod, small boat attacks on an oil platform in Al Basra and the French oil tanker *Limberg*, and the transportation of suspected terrorist operatives via containers in Italy."[46]

So far, the main action taken by the DHS to prevent a nuclear attack in the United States is the deployment of direct detection systems on site in local ports. The Department, through the CBP and the USCG, has spent $300 million to install 470 radiation portal monitors (RPMs)—a technology meant to detect nuclear and dirty bombs—at U.S. points of entry.[47] And President Bush's FY2006 budget requested $125 million to purchase additional RPMs.[48]

To further prevention efforts, President Bush's FY2006 budget request also includes $227.3 million to form a Domestic Nuclear Detection Office (DNDO) within DHS.[49] But the House and Senate versions of the FY2006 Homeland Security appropriations bill (HR2360) provide just $127 million for the office.[50]

According to a DHS fact sheet, "The DNDO will provide a single accountable organization with dedicated responsibilities to develop the global nuclear detection architecture, and acquire, and support the deployment of the domestic detection system. The mission of the office addresses a broad spectrum of radiological and nuclear protective measures, but is focused directly on nuclear detection."[51]

DHS is also focusing some of its efforts on foreign ports. For instance, it is trying to forge relationships with foreign ports to implement container security programs. The FY2006 budget provides $138.8 million for this purpose, including $5.4 million in new funding to expand the Container Security Initiative (CSI), a program administered by CBP.[52] The CSI was implemented to target high-risk containers for inspection at overseas ports prior to their departure for U.S. ports. To that effect, CSI deploys teams of inspectors, special agents, and intelligence analysts to foreign "megaports" and other strategic ports to inspect containerized cargo for weapons of mass destruction before it is ever shipped to the United States. The CSI has now put Customs officers in 38 ports overseas to monitor containers as they are being loaded.[53]

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is another program put in place by the DHS and CBP to improve cargo security while facilitating commerce. C-TPAT will receive $54.3 million in FY2006.[54] This program is meant to strengthen the Department of Homeland Security's partnerships with foreign manufacturers and importers. These partners—7,000 to date—agree to meet "supply chain" standards for establishing a secure chain of custody for every unit of cargo traded overseas. This would ensure that their shipment methods repel potential terrorist attempts to use those shipments for introducing weapons of mass destruction into our ports.

Finally, the U.S. Government is also tackling the nuclear threat by trying to secure the weapons and highly dangerous materials scattered mainly in Russia and other countries of the former Soviet Union. This spending is not specifically port security related. However, considering the high probability that dangerous materials would be brought into the United States through our ports and the fact that securing them is a first best solution, this spending should be included in this section.

The government's main instrument in this area is the Cooperative Threat Reduction Program—usually referred to as "Nunn-Lugar," after the senators who

sponsored the legislation in 1991. Today, the U.S. government has dozens of separate programs, in several cabinet departments, in charge of keeping nuclear weapons and weapon-usable nuclear materials out of terrorists' hands. Activities in these programs include securing and accounting for vulnerable nuclear material, helping states intercept nuclear smugglers at their borders, and getting rid of vulnerable caches of bomb material.

In his February 7, 2005 budget proposal, President Bush called for a modest increase in federal spending for such programs that work to secure and dismantle WMD and related materials worldwide and for an expansion of funding for activities outside Russia and the former Soviet Union. Table 4 shows the change in funding for nuclear threat reduction programs since President Bush took office.

Table 4. Change in Nonproliferation Funding between FY2001 and F2006 ($million)

Departements	FY2001 enacted	FY2006 Proposed	$ Change 2001-2006	% Change 2001-2006
Department of Defense	410.3	415.6	5.3	1.3%
Departement of Energy	518	720	202	39.0%
Department of State	261	161.1	-99.9	-38.3%
Department of Homeland Security	0	0	0	0
Total	1189.3	1296.7	107.4	9.0%

Source: Budget of the United States FY2006, Willian Hoehn's "Preliminary Analysis of the US Department of Energy's FY2006 Budget Requests" and "Preliminary Analysis of the US State Department 's FY2006 Budget Requests"and the Russian American Nuclear Security Advisory Council.

The bulk of the proposed spending is spread between three departments: the Department of Defense (DOD), the Department of Energy (DOE) and the State Department. Through the DOD, the administration's fiscal year 2006 budget request proposes allocating $415.6 million to the Pentagon's Cooperative Threat Reduction (CTR) program, less than a 2 percent increase from the $409 million appropriated in 2005.[55]

The administration's FY2006 request for DOE's National Nuclear Security Administration (NNSA) includes $526 million for threat reduction activities in Russia and states of the former Soviet Union, signaling an increase of nearly 20 percent from the $439 million requested in 2005.[56] By some calculations, the request is $720 million if related programs that operate outside the former Soviet Union are included.[57]

However, these numbers might be misleading. Part of the DOE budget includes disposition of fissile materials in US and in Russia. Yet according to Nuclear Threat Initiative (NTI) expert Laura Holgate, the biggest share of that effort is to support activities in the US to eliminate our own HEU and plutonium; while only $64M of that is for work in Russia. In other words, the vast majority of the DOE budget growth has to do with the increasing funds needed to construct facilities in the US, rather than an increase in activity in Russia and elsewhere. Of course, the funds spent for plutonium disposition in the US do represent contributions to our overall national security in that they are directly linked to progress in Russian plutonium disposition so US expenditures probably are appropriate or necessary, but they distort the aggregate funding levels in ways that allow the administration to take credit for increases that aren't actually reflective of increased effort overseas.

According to William Hoelm (2005), the State Department's threat reduction efforts in the former Soviet Union would receive $71 million, the same amount appropriated in fiscal year 2005.[58] The Nonproliferation of WMD Expertise program is the largest State Department budget item for these activities and may receive $52.6 million for fiscal year 2006, an increase of about $2.5 million over current spending. Previously known as Science Centers/Bio Redirection, this program engages and redirects former weapons scientists into peaceful research and civilian work worldwide.[59] The budget also allots $37.5 million to the Nonproliferation and Disarmament Fund (NDF), an increase of about $5.7 million from fiscal year 2005. The NDF is the State Department's quick-response mechanism for nonproliferation, allocating funds on an as-needed basis to projects overseas that counter new or emerging proliferation threats.[60]

To summarize, in the best case scenario the Bush administration has proposed spending roughly $1.7 billion in FY2006 to prevent WMD incidents in the United States. Most of that effort—$1.2 billion—will be conducted outside of DHS through DOE and DOD's cooperative nonproliferation projects and very little of that amount actually goes to protection of fissile material stockpiles overseas. DHS will receive $352 million to spend on direct detection systems in U.S. ports and $194 million on detection in foreign ports.

III. 2. Is DHS Achieving Its Objectives?

III. 2. a. The Port Security Grant Program

The stated objective of the Port Security Grant Program is to fund security upgrades to help protect ports in case of a terrorist attack. According to an estimate by the Coast Guard, the cost for enhancing security at America's 361 maritime facilities would be $1.5 billion in the first year, plus an additional $7.3 billion over the next decade.[61] Thus, if the goal is to enhance security in our ports, $140.9 million is likely to be inadequate. That remains true even if we include the $706 million in direct grants already allocated to ports to improve their physical and operational security and spending.[62]

In addition, critics have argued that the U.S. port infrastructure is so vast that spreading $140.9 million across the entire nation will not achieve meaningful security either. On the other hand, considering the narrow and specific focus of the grant program, one can argue that there is a limit to how many video surveillance cameras are needed to secure the country and thus four years after the program started, very little money needs to be allocated now to fill that objective.

More substantive criticism came from within the Department of Homeland Security. A review of four separate rounds of the Port Security Grant Program conducted by the DHS Inspector General (IG) between December 2003 and May 2004 questioned the merits of hundreds of projects funded with these grants, ultimately raising doubts about the ability of the program to achieve any meaningful security.[63]

The grant system is meant to be a competitive grant allocation program. In theory, grants are given out based the merits and the expected security returns of applications submitted by individual ports. However, the IG reports that "[t]he program funded projects despite dubious scores by its evaluators against key criteria, raising questions about the merits of several hundred projects."[64] For instance, more than $130,000 was awarded to a port for a closed-circuit television system even after the field reviewers ranked the project 27th of 29 applications and stated in its internal review documents that

"these initiatives would be redundant to what the port authority has in place."[65] A $25,000 grant was awarded to install video surveillance equipment and alarms at a port next to a luxury entertainment complex that included restaurants, a hotel, and a spa, even though this project was ranked last among the applications.[66]

Given the limited budget available, the funding of such low-priority projects necessarily means that the reverse situation also occurred: many projects were not funded despite strong support from the field review. For instance, in round three, no grants were awarded to 54 projects that were ranked highly, i.e., in the top five of their groups.[67]

Private entities also applied for, and received, substantial funding. [68] There, the IG also reported that funds went to projects that were rated below average or worse during the evaluation process, calling into question the merits of these projects.[69] For instance, in rounds two and three, 155 private-sector projects that ranked below average or worse were funded at a cost of $32.4 million.[70]

Furthermore, many port security grant recipients have not spent the funds awarded to them: after the first three rounds of grants, including the Urban Area Security Initiative, recipients have spent only 21 percent of the total amount awarded ($107 million out of $515 million).[71]

When the grant funds have been spent, the IG reports some questionable uses of the money. For instance, many grants were given to port security projects that "appeared to be for a purpose other than security against an act of terrorism."[72] Here are some examples:

- $351,000 awarded to a port to buy a mobile command center that DHS's field reviewers said "appears to be a luxury item."[73]
- $10,000 given to one port for encrypted radios that the DHS field staff concluded were not needed and perhaps not compatible with the federal and state radios.[74]
- $935,000 awarded to a port where an industrial park was being built, leading the Department staff members to question if the money was in fact an economic grant instead of anti-terrorism financing.[75]
- $1,060,000 awarded to a port for fortified crash beams even though the Department field reviewers believed that this project was primarily anti-theft, not anti-terrorism.[76]

In the end, the IG's report on the Port Security Grant Program concludes that the Department has "no assurance that the program is protecting the nation's most critical and vulnerable port infrastructure and assets."[77]

Accordingly, reform of the grant system is a worthy priority. The good news is that DHS's Office of Domestic Preparedness, newly in charge of the PSGP allocation, announced in May 2005 that the program was going to be completely revamped so that money would be distributed using a risk-based formula based on the elements of threat, vulnerability, and consequence.

Previously, DHS had tried to spread funds to as many applicants as possible, leading to 361 ports receiving security grants. In FY2005, The Nations; 129 largest ports were evaluated using risks elements. Based on ODP's evaluation, only 66 port areas have been identified as eligible. Successful applicants will be awarded through a competitive process. This is a tremendous improvement.

Another interest aspect of the reform is the fact that private companies receiving grants will be asked to match 50 percent of the grants with their own money placing the incentive for the private company in the right place.

Hopefully though, ODP's next productive step will be the termination of the Port Security Grant Program.

III.2.b. Counter-WMD activities

In spite of a lower probability of occurrence than other possible attacks, the consequences of nuclear or radiological terrorism would be so devastating (see tables 1 and 2) that it is the one threat that requires zero tolerance.

Unfortunately, DHS's main domestic line of defense against the nuclear threat—the RPMs—has so far proven unreliable. On June 21, 2005, a panel of nuclear-security experts told members of the House Homeland Security Committee that the monitors cannot reliably detect highly-enriched uranium, the crucial element in a nuclear bomb.[78] Terrorists could easily shield the uranium and avoid detection.

According to experts, another limitation of the monitoring system is one of discrimination. Specifically, today's equipment lacks a refined capability to rapidly determine the type of radioactive materials it detects, which leads to higher "nuisance alarm" rates—the number of alarms that must be resolved by further inspection.[79] In the Port Authority of New York and New Jersey, for instance, 22 monitors are used to screen 45 percent of containers, emitting about 150 false alarms a day. This means that once the port starts screening 100 percent of cargo, over 300 false alarms a day will sound.[80]

Each false alarm must be investigated, which exacts a high cost in terms of time, money, and security. Based on an extremely conservative estimate of 10 minutes per follow-up inspection—and assuming that monitor operations are fully staffed—investigating 300 false alarms a day would take at least 50 man-hours per day. Since 95 percent of international goods that come into the country enter through America's 361 ports, screening all cargo with RPMs could drastically slow down shipping. The negative economic impact could be immense. The security impact could also be significant: as a consequence of the already-high false alarm costs, some port officials have decreased the detection sensitivity of the radiation monitors to cut down on the number of disturbances, further reducing the probability of detecting dangerous devices.

Technology is only as effective as the people operating it. Even if radiation detection were 100 percent effective, it would be constrained by the lack of competent personnel to operate them. Some reports also point to border agents improperly handling radiation detectors.[81]

On the whole, the cost effectiveness of RPMs seems dubious. Moreover, even if the system could detect every type of nuclear material, it would be useless if terrorists did not bring the nuclear devices through the fixed ports of entry where the monitors are usually located. In fact, it would be easy for terrorists to evade the RPMs by shipping a nuclear weapon—whole or in parts—on a yacht or in a truck, or even by carrying it in piece by piece in backpacks, or smuggling it across any number of unprotected sections of the northern and southern borders.[82] In the June edition of *National Journal*, journalists Gorman and Freedberg added that "Uranium, ironically, is so low in radioactivity that it is safe to handle without gloves, so a bomb's worth could even be broken in hundreds of half-pound chunks and smuggled into the country in people's pockets."[83]

To address these concerns, DNDO recently announced that it was looking for cutting edge technologies to thwart the illicit shipment of nuclear materials.[84] The agency is asking companies to suggest ideas for mobilizing detectors so they can fit in police officers' pockets or pick up on radioactive materials while in the trunk of a moving police car. The idea is to keep terrorists guessing by deploying detectors at unexpected and changing places. Another new technology would be able to pick up small amount of radiation over long period of time.

In addition to its troubles with domestic inspection programs, DHS is also experiencing difficulties with its foreign programs, CSI and C-TAPT. In May 2005, the U.S. Senate Permanent Subcommittee on Investigations, led by Senator Norm Coleman (R-MN), in conjunction with Senator Carl Levin (D-MI), Senator Susan Collins (R-ME), Senator Joe Lieberman (D-CT), and Representative John Dingell (D-MI), released two critical Government Accountability Office (GAO) reports detailing problems with these two key homeland security cargo security programs. These two GAO reports are the most recent in a series that have found crippling flaws in Customs' programs.

The GAO reports that the verification process for applications to the C-TPAT program does not provide "an actual verification that the supply chain security measures contained in the member's security profile are accurate and are being followed before CBP grants the member benefits."[85] Other weaknesses in the program "limit [CBP's] ability to ensure that the program supports the prevention of terrorists and terrorist weapons from entering the United States."[86]

In addition, GAO explains how "staffing imbalances" have impeded the ability of CSI ports to target all U.S.-bound shipments.[87] GAO cites "political and practical considerations" that have made it difficult for Customs to develop a model to determine the required level of staff. It appears that the National Treasury Employees Union (NTEU) has more to say about where and when Customs inspectors work than management does. As a result, 35 percent of U.S.-bound shipments from CSI ports were not inspected.

The Subcommittee's oversight investigation confirmed these problems and specifically identified the following shortcomings: CBP inspects 34 percent of containers overseas, but inspects only 17.5 percent of high-risk cargo. In addition, the equipment used overseas, such as nuclear detection devices and non-intrusive inspection machines, is untested and of unknown reliability; substantial benefits, including fewer inspections, are provided to certified C-TPAT importers without a thorough validation of their supply chain security; and of those validations that do occur, the process lacks any rigor or independence.[88]

Two recent smuggling incidents demonstrate the inherent vulnerabilities in the global supply chain. On January 15, 2005 and again on April 2, 2005, upwards of 30 Chinese immigrants were found emerging from containers arriving at the Port of Los Angeles.[89] These incidents aggravate security experts' concerns that containers could hold members of terrorist organizations and/or weapons of mass destruction.

An additional weakness in inspections is highlighted by a new DHS Inspector General report that concludes that there is room for much improvement in the Automated Targeting System (ATS), the Department's intelligence system to mark high risk oceangoing containers for further inspections.[90] Approximately 9 million oceangoing cargo containers arrive annually at seaports in the U.S., making it impossible to

physically inspect each container without hampering the flow of commerce. Inspectors at overseas CSI ports and at U.S. seaports use ATS to assess the risk associated with each container and determine which containers will undergo inspections.

In theory, through this system, intelligence is used to screen information on 100 percent of the cargo going to the U.S. ATS is also a major component of the Department's efforts to prevent terrorists from sabotaging shipping containers. However, the IG's report questions the completeness and accuracy of the cargo manifests that ATS uses and raises doubts about whether the system is drawing enough shipping data to make accurate risk assessments.

The Department of Homeland Security is not the only cabinet department trying to secure maritime cargo. In the last ten years, some $500 million was allocated by Congress to the Department of Energy to run a parallel port security initiative called Megaports that installs radiation detectors to screen cargo containers at the largest foreign ports.[91] Unfortunately, the centerpiece of every Megaport installation is the radiation portal monitor that, as described above, is less than effective.[92]

Also, testifying before Congress in June, a GAO representative testified that "the common problem faced by the U.S. programs to combat nuclear smuggling is the lack of effective planning and coordination among responsible agencies."[93] The good news is that a government-wide plan to guide U.S. efforts is on its way and some of the many duplicative programs are being consolidated. However, at the domestic level, DHS still fails to coordinate with other agencies on longer-term objectives such as attempting to improve the radiation detection technology used in portal monitors.[94]

Finally, according to the 9/11 Commission, outside experts are deeply worried about the U.S. Government's commitment and approach to securing the weapons and fissile materials scattered around the world.[95] The commission members report that the Cooperative Threat Reduction Program is in dire need of serious expansion, improvement, and resources.[96] Even though DHS is not involved in that effort directly, the Department should be highly interested in the success and efficiency of the nuclear threat reduction program. Its failures expose the country to great risks and puts more pressure on the other lines of defense put in place by DHS.

III. 3. Should DHS and the Federal Government Be Prioritizing Different Objectives for Port Security?

III. 3. a. The Port Security Grant Program

As explained in section II, the most cost effective measures to protect ports from direct attacks are those aimed at preventing bad things from happening inside our ports. The Port Security Grant Program, however, is predicated on the notion of turning each port into a little Maginot line instead of preventing the next terrorist attack. In that sense, the program is not making us safer.

To be sure, because not every attack can be prevented, some level of direct defense, such as physical barriers (e.g., fences), surveillance equipment (e.g., closed-circuit television), and access control systems for employees and visitors, is wise. But if funds are going to be spent to upgrade security in ports, it should be done in a cost efficient way. It means that the money should go to critical national ports and terminals, the areas of highest consequence with the greatest vulnerability to terrorist attack.

As already mentioned, 95 percent of non-North-American trade enters the United States through the nation's 361 public and private ports and about 42 percent of that trade moves through just 10 ports, with the biggest loads passing though Houston, New York, and South Louisiana.[97] In addition, over 40 percent of cargo and 25 percent of refined energy coming into the country goes through the twin ports of Los Angeles and Long Beach.

Severely damaging one of these critical ports could not only cause injuries, death, and property damage, but could also disrupt the flow of basic goods into and out of the country. For this reason, the nation's biggest ports are regarded as high-risk areas. However, they often receive relatively less grant money than smaller and lower-risk ports.

Table 3 shows how much in dollars per ton each state received from the Port Security Grant Program over the last three years (i.e., excluding the $75 million made available under the Urban Area Security Initiative).

The states with the biggest loads passing through their ports are Louisiana, Texas, New York, and California. Nearly 53 percent of all trade moves through these four states.[98] Louisiana received 10 percent of general grant money while its trade accounts for 16 percent of the nation's commerce. Texas received 13 percent of general grant money while its trade tonnage accounts for 16 percent of the nation's commerce. And Guam, which accounts for 0.01 percent of the nation's commerce, receives 0.16 percent of all the grant monies. This translates to $0.105 per ton in Louisiana, $0.137 per ton in Texas and $3.196 per ton in Guam.

Table 3. Dollars Per Ton Each State Received from Port Security Grant Programs Over the Last Three Years

State	Dollars per Ton	State	Dollars per Ton
Guam	3.196	Louisiana	0.105
North Carolina	0.865	Oregon	0.090
Hawaii	0.527	New Jersey	0.088
California	0.428	Pennsylvania	0.080
Massachusetts	0.400	Mississippi	0.074
Georgia	0.386	Illinois	0.070
Florida	0.385	District of Columbia	0.060
Connecticut	0.380	Virgin Islands	0.056
New Hampshire	0.348	Tennessee	0.048
South Carolina	0.333	Alabama	0.039
Maryland	0.303	Ohio	0.039
Washington	0.295	West Virginia	0.034
Virginia	0.293	Michigan	0.024
Rhode Island	0.288	Minnesota	0.020
New York	0.272	Delaware	0.019
Puerto Rico	0.250	Missouri	0.016
Oklahoma	0.242	Kentucky	0.016
Texas	0.137	Indiana	0.014
Kansas	0.131	Iowa	0.004
Maine	0.109	Wisconsin	0.002
Alaska	0.105		

Source: Author's calculation based on American Association of Port Authorities website: http://www.aapa-ports.org/govrelations/issues/crime.htm and the Army Corps of Engineers (2003 figures): http://www.iwr.usace.army.mil/ndc/wcsc/stateton03.htm
Note: Mariana Islands-Saipan and Vermont are not included because no waterbone cargo data was available. Mariana received a total of $2,129,577 and Vermont received $131,232.

Again, the DHS Inspector General's audit of the Port Security Grant Program confirms this vast problem of misplaced priorities. It explains that the Department has put too much emphasis on spreading money around broadly, instead of directing it toward the most vulnerable and important targets or toward cost effective security measures. According to the audit, "Grant award decisions are made with the intent of expending all available funding and spreading funds to as many applicants as possible."[99] During the third round, selection officials even capped funding per entity and per award in order to reach more applicants and projects.[100]

Consequently, hundred of thousands of dollars were spent on low-traffic ports defined as low-risk areas by DHS's own standards. Major ports such as New York, Los Angeles, Houston, and South Louisiana received large allocations, but DHS also awarded smaller grants to ports such as Christiansted in the Virgin Islands, Martha's Vineyard in Massachusetts, Tulsa Port of Catoosa in Oklahoma, and six ports in Alaska, none of which appeared to meet the grant eligibility requirements.[101] For example, $180,000 was awarded to a port that the field review team described as a "small remote facility that receives less than 20 ships a year."[102]

As explained in the previous section, however, there is good news. The Office of Domestic Preparedness' new design of the grant system addresses most of these criticisms and directs the spending to high-risk, high-vulnerability ports rather than spreading a little money to every port as it did in the past.

Despite this policy improvement, a more fundamental issue still needs to be addressed: whether the federal government should even be involved in upgrading port security. Public seaports are generally owned and operated by local governments through a port authority; however, large portions of seaport real estate are leased to the private sector with the local government operating as a landlord. In addition, there are many privately owned and operated terminals within seaports that exist independently of the local port authority. Where do the private, state, and local sectors' responsibilities for preventing terrorism end and where does the federal government's begin?

As mentioned earlier, none of the prevention techniques used in ports is a public good: the cost to the port would be the same as the cost to the government. And as with other government spending, the local or private decision-maker is in a better position to determine local needs and the most effective way to meet them. Accordingly, all such spending should be local, e.g., paid for from taxes and fees charged by the port in question.

Having port authorities and the private sector responsible for the direct defense of ports would guarantee a more responsible use of the money. When port security is federalized, a given port authority official and the state's Congressmen have no incentive to admit that the port is not a likely target or that if it ever were a target, damages would be limited. By contrast, when port security programs are the responsibility of states and port authorities, officials have an incentive to assess risk and potential damages accurately.

Moreover, once port security is the responsibility of port authorities, they have an incentive to identify the most cost effective measures. They are also the best suited to identify how much should be spent on each measure. If, for instance, they measure that the biggest expected cost from an attack is not the loss of the inventory stored in the port but the number of days that the port is unable to operate, port authorities will lower the expected damage by developing plans for the aftermath of an attack. They will focus on evacuating civilians and personnel, placing emergency equipment within easy reach, training personnel to handle emergencies and attacks, and planning for business continuity to allow the port to get up and running quickly after an attack.

Given these factors, the PSGP is probably a misuse of our federal dollars. The good news is that it remains rather small. The even better news is that the administration and DHS are trying to reform the PSGP. In his FY2006 budget, President Bush proposes consolidating multiple narrowly-focused programs (PSGP, Transit/Rail Security, Intercity Bus, Trucking Industry Security, and Buffer Zone Protection) into a Target Infrastructure Protection Program (TIPP).

One of the main benefits of TIPP is that it would effectively guarantee that no more money will be spent on security equipment for ports in general and for low risk ports in particular, unless intelligence demonstrates that DHS needs to focus on the maritime system in a given year. Moreover, the creation of this single grant program for targeted infrastructure would allow DHS the flexibility to allocate grants based on the most recent threat information, thus addressing emerging needs and national priorities.

Today, Congress allocates funding based on a knee-jerk reaction to the news of the day. For instance, after the July 7, 2005 subway bombing in London, some members of Congress proposed boosting transit system funds from $50 million to $1.2 billion. This ad hoc method of targeting security funds is an ineffective way to address terrorist threats. Over a year might pass between the time when the President makes his budget requests and the time when Congress appropriates the funds. By then, the risk might be somewhere else, or it might even be too late. If terrorists are in fact now interested in bombing subways in the U.S., by the time the transit system receives the extra millions allocated to address that threat, terrorists would have had the time to plan and undertake many alternative actions.

The administration's TIPP proposal would address this problem by having one flexible source of money to allocate to the places or industries where intelligence reports say the threat is. Congress would have to move away from giving funds to a specific industry year after year. It would prevent industries from developing the entitlement mentality born of receiving federal funds on a regular basis, independently of security needs or risks.

Funding for the existing homeland security programs in FY2005 was $365 million. The President's FY2006 budget request for TIPP, which combines those programs, is $600 million—more than a 50 percent increase. Yet, members of Congress and the special interests involved are resisting this worthy reform, placing politics above security. As is often the case, politicians are more interested in being able to tell their constituents what they have done for a specific industry rather than explaining that they have improved the Secretary's ability to distribute homeland security funds efficiently.

III.1.b. Counter-WMD activities

As explained in section II, the consequences of WMD materials entering through ports could be much more serious than the damage from direct attacks on ports. The best ways to protect against WMD are, listed in descending order: (1) control stockpiles of fissile material, (2) gather intelligence on planned attacks, (3) prevent dangerous material from being loaded into U.S.-bound cargo vessels, and (4) detect WMD material upon entry into a U.S. port. The public-good aspects of all four of these preventive techniques make them naturally the purview of the federal government.

Unfortunately, it seems that DHS's effort so far has been to invest primarily in the least attractive solution, (4). DHS has focused on increasing direct detection on site in U.S. ports, mainly through the use of radiation portal monitors, which, as we have explained, do not effectively detect WMD material.

But even if DHS were to acquire cutting-edge technologies that would significantly increase the probability of detecting dangerous materials, direct detection on site in local ports would remain the least cost effective protection measure.

First, because it is the last line of defense, if the system fails just once, the dangerous material or the bomb would be inside the country, making it almost impossible to prevent the worst. More importantly, if terrorists cannot smuggle a nuclear weapon inside the country through our ports, their next best option would probably be to blow up the bomb immediately upon arrival in the port. This would have devastating

consequences too, especially considering that terrorists would probably target the largest ports to create the maximum level of destruction.

The existence of devastating alternatives make this line of defense the least cost effective measure. Yet DHS has already spent $300 million on these monitors and plans to spend an addition $125 million. Making their acquisition, monitoring, and operation the DNDO's main focus costs another $227 million. And these numbers do not even include the money invested by DOD and DOE.

A more effective measure is to stop terrorists from bringing a WMD anywhere near our ports. This is achieved by spotting suspicious anomalies while cargos are in foreign ports. Because foreign governments, especially those that are very unlikely terrorist targets, have almost no incentive to invest money to tighten security in their ports to protect U.S. ports, DHS should provide most of the funding.

DHS will be spending roughly $194 million in FY2006 through its CSI and C-TAPT programs to secure cargo coming to the U.S. from foreign ports. That's close to half the amount spent on direct detection in U.S. ports, a much less effective alternative.

According to experts, the level and depth of the investment spent on screening efforts in foreign ports are insufficient. Port security expert Stephen Flynn estimates that deploying a screening system that would run every container through both radiation and gamma-ray density sensors (which would detect shielding efforts on the part of terrorists) and then take a picture of the container's identification numbers to match against databases for additional screening at every port in the world would cost roughly $1.5 billion.[103]

Buying many more radiation portal monitors will not come close to securing the country against WMD attacks. Instead, DHS should expand its partnerships with foreign ports. It should also encourage public-private partnerships that adopt sustainable and effective port-security programs in foreign ports. For instance, over the last year such a system was put in place by the private members of the Hong Kong Container Terminal Operators. Their goal is to enhance container-screening security while at the same time minimizing the effect of the cargo inspection regime on the efficiency of operation and the flow of cargo. Thus far, the system has proven quite successful in screening 100 percent of U.S,-bound cargo loaded in Hong Kong while minimizing the delays when shipments required more thorough inspection. They have offered to work with DHS to improve and implement this same system around the world.

But let's imagine that DHS effectively secures the cargo of a ship en route to the U.S. so that no nuclear weapons are introduced in the cargo after departure from the foreign port. The probability of successfully using the maritime system to cause nuclear damage in the U.S. or in a U.S. port is significantly reduced. It means that terrorists have a strong incentive to find an alternative to introduce nuclear materials into the U.S. They can try to smuggle it through the Canadian or Mexican borders in trucks. They can try to hide the nuclear material in a plane. They can leverage the techniques used by the drug dealers who introduce hundreds of metric tons of cocaine and heroin into the United States each year.

If it becomes too difficult to target the United States, terrorists can try to blow up a city in a country with close ties to the United States. Ultimately, the most cost-effective measure to prevent nuclear incidents that would affect the United States is to stop terrorists from acquiring nuclear materials in the first place. Without fissile materials,

terrorists cannot build nuclear or dirty bombs. However, once they have put their hands on such material, each of the later lines of defense is more desperate and more doubtful. Bunn, Wire, and Holdren (2003) comment, "Indeed, if defenses against nuclear weapons at the U.S. border or within the United States are ever called into play, this will represent a serious failure of U.S. policy, in failing to intercept the threat earlier in the terrorist pathway to the bomb."[104]

As mentioned earlier, the Bush administration has proposed spending roughly $1.2 billion in FY2006 on nuclear threat reduction programs abroad. Unfortunately, according to Nuclear Threat Initiative expert Laura Holgate, "today [the actual protection of global fissile material] gets only a mere fraction of the $1 billion spent on cooperative nonproliferation projects, and those funds only address a fraction of the fissile material in the world." The budget for protecting stockpiles is estimated at $250 million per year.[105] If that number is accurate, it is only slightly higher than what DHS spent to secure cargos in foreign ports and less than what it spent to install radiation portal monitors in U.S. ports. This is a flagrant demonstration of misplaced priorities government wide but also within DHS.

It is also quite dangerous. Today, most of the current fissile material security costs outside the U.S. are borne by the nations holding those stocks. Whether we can be confident that all nations have the resources, the incentives, and the political will to carry out adequate security on an ongoing basis is a real concern. If they do not, these countries will under-invest in stockpile protection, which will in turn increase the probability that terrorists could acquire dangerous materials.

According to Holgate, there is no good cost estimate for the total cost of sustainable security for global fissile material stockpiles. However, our current spending is nowhere near what would be needed to achieve that task. Mathieu Bunn, of the Carnegie Endowment for International Peace, estimates that $1.5 billion a year would be necessary. [106] She adds that "the most quotable figure to adequately address the Russian aspects of nuclear insecurity came from the Baker-Cutler report in January 2001 as part of the Secretary of Energy Advisory Board, and they used a figure of $30 billion over 10 years." Recently, the 9/11 Commission members have been using this $3 billion a year figure to stress the lack of resources devoted to the WMD threat, but Holgate cautions us that the figure is a guess, with no analytical back-up, and leaves out nuclear security issues elsewhere in the world.[107]

Finally, to prevent the next terrorist attack, good intelligence is absolutely fundamental. Coast Guard assets support many missions aimed at keeping terrorists out of our ports. Since September 11, the Coast Guard's homeland security missions have greatly expanded. Today, 47 percent of the Coast Guard's operating expenses fund homeland security activities.[108] The Coast Guard's budget request for FY2006 is $8.1 billion. Out of the $5.5 billion requested for the Operating Expenses (OE) account that finances daily operations, $2.6 billion goes to the Cost Guard's five homeland security missions. [109] And $1.5 billion will be directed to port security.[110]That's 28 percent of the OE and 19 percent of the Coast Guard's budget.

Unfortunately, the Coast Guard's equipment is aging and/or obsolete. In 1998, a modernization and recapitalization program called Integrated Deepwater System was launched as a $24 billion 25-year plan to replace the fleet.[111] In February 2005, President Bush requested $966 million for the Deepwater Program but the House FY2006

appropriations bill (HR2360), which passed in May, provides only $500 million.[112] The Senate version of the appropriations bill (S Rept 109-83) that passed in July allotted $900 million.[113]

Here Congress demonstrates a lack of strategic spending. Instead of pouring money into port grants and radiation portal monitors whose contribution to overall maritime security is unclear, we should ensure that the Deepwater Program is fully funded so the Coast Guard can perform its most important mission: securing ports from terrorist attacks.

One option for achieving full funding would be to privatize all non-homeland security Coast Guard missions such as maritime safety, maritime mobility, or maritime environment protection. These functions are best left to state and local governments or the private sector. Privatizing or turning these functions over to the states would free $4.2 billion that could be directed to fund homeland security priorities.[114]

To conclude, DHS and the federal government's priorities seem to be misplaced. As explained earlier, the first best strategy is to protect the stockpiles of fissile materials from being stolen by terrorists in the first place. This of course is not easy. There are several hundred tons of highly-enriched uranium in Russia alone, and additional tons are scattered throughout dozens of countries. Yet, government-wide we spend a total of only $250 million on this effort specifically. Including all nuclear threat reduction programs, the U.S. government spends roughly $1.2 billion, mainly in Russia and the former Soviet Union.

The related second best solution is to collect intelligence on who is trying to acquire fissile material or on potential terrorist attacks. It is hard to estimate the current spending on this effort. However, we do know that the Coast Guard could be a key player, but Congress is reluctant to fund the modernization of its decaying assets.

The third best solution is to place security mechanisms in foreign ports to prevent nuclear devices from arriving in the United States. Yet, DHS spends $352 million on this least cost effective solution, while spending only $194 million in foreign port security.

III.4. Prioritizing port security within homeland security

The same logic used to set port security spending and objectives can be used to measure the port security threats against other homeland security threats. Because the various sectors in the U.S. that are vulnerable to terrorist attack are competing for limited anti-terrorism dollars, we should allocate funds based on careful, risk-based analysis.

If experts are correct, the threat of WMD materials being transported through a port is the largest homeland security risk we face. The worst-case WMD scenario is the destruction of a city like New York, costing over $1 trillion and hundreds of thousands of lives (see Section II, table 1). This outcome is much more devastating than other worst-case scenarios, yet spending on port security pales in comparison to spending on other programs that address lower risks.

For example, in airline security, improved cockpit security has limited the worst-case scenario to the destruction of a plane and loss of approximately 300 passengers. We will spend $4.7 on baggage screening for airlines in FY2006, but $2 billion on port security. More importantly, of that money DHS will spend $500 million directly protecting the United States against import of WMD.

DHS will also spend over $2.8 billion in FY2006 to help state and local government build their response capacity.[115] Yet, the first responder grant programs are predicated on the notion of cleaning up after terrorists successfully attacked. They are not making us more secure. Furthermore, nuclear experts predict that these investments will be irrelevant if we are actually attacked with a WMD weapon.[116]

Of course, the assessment of the nuclear threat and the priority placed on port security rest mainly on the probability of such a threat. If DHS estimates that the probability of a terrorist attack with an actual nuclear weapon is very small, it might be cost effective to spend significantly more on other threats. Yet, the case can be made that even if the probability of nuclear threat is lower than the probability of virtually any other type of terrorist attacks, the devastation from such an attack would be so overwhelming that this threat—defined as the probability multiplied by the consequences—must be considered one of the greatest dangers America faces. In that case, we should decrease spending on airline security and other low risk/low productivity activities to shift some of that spending on counter-WMD port security.

As with port security, the best defense against terrorism overall is to stop it at the source. As such, we should radically shift priorities toward intelligence. But we should also shift resources to protect our country against the most devastating threat of all: WMD attacks on U.S. soil. Yet, for years now protecting stockpiles of fissile materials has been and remains a low priority for the administration.

It is troubling how in the last ten years, efforts by Sen. Richard Lugar (R-Ind.) to accelerate the pace and expand the scope of related U.S. nonproliferation missions are systematically and consistently met with resistance by Congress. [117] Congressmen have been more interested in bringing back visible spending items, such as hazmat suits and fire trucks, than protecting fissile material stockpiles materials abroad. Similarly, Congress has been more interested in spending money on port security grants and radiation portal monitors than on foreign ports. Unfortunately, Congress's reluctance is consistent with reports that these efforts have not really been championed by the White House.[118]

Another troubling tradeoff made within the homeland security budget is the reluctance to properly fund the Deepwater Program while funding many items that should be left to the states and the private sector to fund—including the Coast Guard's non homeland security activities. Investments in espionage, intelligence, and immigration control benefit all the states and should be made by the federal government. But the benefits of protection of public infrastructure like bridges, transit systems and water treatment plants are enjoyed by the residents of a particular state, rather than many states, so these investments should be made at the state level.

As mentioned earlier, many of the Coast Guard's assets are used for intelligence and to help prevent the next terrorist attacks. If these assets are deteriorating to the point of becoming useless, it seems like a good investment to replace them. Yet, House DHS appropriators, led by Congressman Rogers are holding firm to their intent to cut Deepwater FY2006 budget to $500 million instead of the $960 requested by the President.

Rep. Rogers professes publicly that his concerns center on the inadequacy of the information the Coast Guard has provided about its program. Yet, hearing records show that the Congressman and his staff have been provided with volumes of detailed

information addressing his concerns. Rep. Rogers also claims that the Coast Guard is recommending a program that is a "Cadillac Seville" when a "Chevrolet" is needed.[119] But, the current program's build out is much smaller by comparison to the CNA or RAND reports' recommendations on the Deepwater Program. Is it possible that some members of Congress feel that, much like the days when the Coast Guard was assigned to the Department of Transportation, the Coast Guard budget can be cut to fund other programs?

In addition, why have no problem funding Coast Guard functions that are non homeland security related up and should not be funded by the federal government to $4 billion a year and be so reluctant to fund functions that could bolster our ability to prevent terrorist attacks? Interestingly, and outside of the homeland security budget, Congress just recently approved a $24 billion spending in the form of 6,000 add-on states projects to the administration's transportation bill but won't fund a legitimate function of the federal government at this level over 25 years.

As for the port security grant program, the level of funding for this item that would be best left to the states and to the private sector is consistent with other such funding. The US transit system security for instance is local and state governments' responsibility. Yet Congress has proposed to allocate $150 million to the Rail and Transit system in FY2006.

To conclude, the evidence of misplaced priorities within port security spending can also be found throughout DHS's budget but also government wide. This of course is mainly the result of Congress's tendency to allocate money based on politics rather than security.

IV. Conclusion

Many terrorism experts believe that maritime container shipping may be an ideal platform to deliver weapons of mass destruction to the United States. If they are correct, intelligence and port security directed at keeping bad things from happening in our ports, along with nuclear detection, should be DHS's priorities within port security spending. Unfortunately, they are not.

Through FY2005, Congress has provided over $650 million in direct grants to ports to improve their physical and operational security and roughly $1.2 billion to nuclear nonproliferation programs, of which only a small portion is directed to protect stockpiles of fissile materials.[120]

More worrisome, much of the money spent on ports goes to projects that should be receiving lower priority. For instance, a large portion of our port security dollars goes to nuclear detection on site, mainly through the implementation and use of radiation portal monitors. Not only has the effectiveness of the monitors often been challenged by experts, but direct detection on site is also by far the least cost effective measure to protect us against the admission of WMD materials into the country. To protect us against WMD attacks in our ports or in our cities, it would be more cost effective to concentrate our resources in foreign ports and in protecting stockpiles of fissile material.

Furthermore, a significant portion of the port security money goes to projects whose contribution to maritime security is unclear. By way of this allocation, many private concerns are using taxpayer funds to secure infrastructure that they should be

securing themselves. Federal dollars should not be used to subsidize ports around the nation.

Instead, Congress and the President should ensure that our intelligence community is effectively engaged in the investigation, interdiction, and elimination of terrorist threats in our ports. In addition, because the Coast Guard supports many missions aimed at keeping terrorists out of our ports, Congress and the President should make sure that its modernization and recapitalization program is appropriately funded.

Finally, if we are going to invest in WMD detection devices, Congress should make sure that this technology is actually capable of detecting the threats it is supposed to detect, including highly enriched uranium. More importantly, the federal government should keep closer tabs on the immense stockpiles of fissile material like highly enriched uranium and plutonium. Until things change, the U.S. will continue to misallocate considerable sums on homeland and port security, yet America will remain vulnerable to catastrophic attack.

Do we really need the deaths of 200,000 people to move this threat to the top of the priority list?

---

[1] Jim Morris (2005), "Don't Worry be Happy: Polls Show Experts More Worried About New Attacks, Americans Less," Congressional Quarterly, June 22.
[2] Stephen E. Flynn (2004), "The Neglected Home Front," Foreign Affairs, September/October.
[3] Council on Foreign relations, "Terrorism: Questions & Answers, Responding to Nuclear Attacks,", http://cfrterrorism.org/security/nuclear.html
[4] John Frittelli, "Maritime Security: Overview of Issues," Congressional Research Service, RS21079, February 24, 2003. http://www.boozman.house.gov/UploadedFiles/TRANS%20-%20Maritime%20Security%20Overview%20of%20Issues.pdf
[5] US Army Corps of Engineers' Navigation Data Center ranks U.S. ports by dollar value and tons of cargo imported and exported. See http://www.iwr.usace.army.mil/ndc.
[6] John Frittelli, "Maritime Security: Overview of Issues," February 24, 2003.
[7] John Frittelli, "Maritime Security: Overview of Issues," February 24, 2003.
[8] U.S. Department of the Treasury. "US Customs Commissioner Robert Bonner, Speech Before the Center for Strategic and International Studies," Washington DC January 17 2002 and Stephen Flynn, America the Vulnerable: How our Government is Failing to Protect us From Terrorism (New York: Harper Collins, 2004), p. 83.
[9] American Association of Port Authorities, "United States Waterborne Foreign Commerce 2003," http://www.aapa-ports.org/industryinfo/statistics.htm.
[10] Ibid.
[11] Ibid.
[12] See for example Gold (1999) for a good review of the literature and a discussion of defense as a public good.
[13] Jim Morris (2005), "Don't Worry be Happy: Polls Show Experts More Worried About New Attacks, Americans Less," Congressional Quarterly, June 22.
[14] Charles D. Ferguson II and William C. Potter (2004), "Terror and Nuclear Threat," San Jose Mercury News, October 10.
[15] National Terror Alert (2004), "CIA Warns Dirty Bomb within Al Qaeda's Capabilities," November 25.
[16] CIA (2003), "Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass destruction and Advanced Conventional Munitions," Attachment A, January. http://www.cia.gov/cia/reports/721_reports/jan_jun2003.htm
[17] Council on Foreign relations, "Terrorism: Questions & Answers, Responding to Nuclear Attacks,", http://cfrterrorism.org/security/nuclear.html
[18] See Area and Population Density from 2000 County and City Data Book.

[19] Aldy, Joseph E. and W. Kip Viscusi (2003). "Age Variations in Workers' Value of Statistical Life," NBER Working Paper No. 10199.
[20] Viscusi, W. Kip (1993). "The Value of Risks to Life and Health," *Journal of Economic Literature* 31(4): 1912-1946.
[21] William C. Thompson Jr. (2002), "One Year Later: The Fiscal Impact of 9/11 on New York City," Office of NYC Comptroller, September 4. http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf
[22] Peter D. Zimmerman and Cheryl Loeb (2004), "Dirty Bomb: The Threat Revisited," Defense Horizons, The Center For Technology And National Security Policy At National Defense University, Number 38, January. http://hps.org/documents/RDD_report.pdf
[23] Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March 2003, http://www.nti.org/e_research/cnwm/cnwm.pdf
[24] William C. Thompson Jr. (2002), "One Year Later: The Fiscal Impact of 9/11 on New York City," Office of NYC Comptroller, September 4. http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf
[25] Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March 2003, p. 18.
[26] Josh Mayer (2003), "Al Qaeda Feared to Have Dirty Bombs," Los Angeles Times, February 8, 2003.
[27] Federation of American Scientists Public Interest report (2002), "Dirty Bomb: response to a Threat," Journal of the federation of American Scientists, Volume 55, Number 2, March/April.
[28] Peter D. Zimmerman and Cheryl Loeb (2004), "Dirty Bomb: The Threat Revisited," Defense Horizons, the Center for Technology And National Security Policy At National Defense University, Number 38, January. http://hps.org/documents/RDD_report.pdf.
[29] William C. Thompson Jr. (2002), "One Year Later: The Fiscal Impact of 9/11 on New York City," Office of NYC Comptroller, September 4. http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf
[30] Stephen E. Flynn (2004), "The Neglected Home Front," Foreign Affairs, September/October.
[31] Joseph F. Bouchard (2005), "Defense in Depth Against Improvised Nuclear Device or radiological Dispersal Device," Zel Tech Technology presentation, April 26.

[32] Barry R. McCaffrey (1997), "Goal: Protect U.S. Borders by Attacking Smuggling and Smuggling-Related Crimes," Office of National Drug Control Policy May 12. www.fas.org/irp/offdocs/iccs/iccsiv.html
[33] Office of National Drug Control Policy (2001), "What America's Users Spend on Illegal Drugs, Trend 1988 to 2000," December, http://www.whitehousedrugpolicy.gov/publications/drugfact/american_users_spend2002/index.html
[34] See Congressional Quarterly. Congressional Transcripts, Congressional Hearings, June 21, 2005, House Homeland Security Subcommittee On Emergency Preparedness, Science And Technology Holds Hearing On Effectiveness Of Nuclear Weapons Detection Technology.
[35] Jim Morris (2005), "Don't Worry be Happy: Polls Show Experts More Worried About New Attacks, Americans Less," Congressional Quarterly, June 22.
[36] Ronald O'Rourke (2005), "Homeland Security: Coast Guard Operations—Background and Issues for Congress," CRS Report for Congress, RS21125, June 30, 2005.
[37] Ronald O'Rourke (2005), "Homeland Security: Coast Guard Operations—Background and Issues for Congress," CRS Report for Congress, RS21125, June 30, 2005.
[38] Author's calculation based on the Budget of the United States, FY2006, the Department of Homeland Security, *Budget in Brief FY2006*, and U.S. Customs and Border Projection, *U.S. Customs and Border Projection FY2006*.
[39] Author's calculation based on *The* Budget *of the United States Government, Fiscal year 2005*, (Washington: Government printing Office, February 2004).
[40] *The* Budget *of the United States Government, Fiscal year 2006*, Appendix, p. 496.

[41] Department of Homeland Security, Budget in Brief FY2004, p. 9. See also Department of Homeland Security, Press Release, "Department of Homeland Security Announces $49 Million in Grants to Secure America's Ports," September 13, 2004.
[42] Office of Inspector General, January 2005, p. 4 and Department of Homeland Security, Press Release, "Department of Homeland Security Announces $49 Million in Grants to Secure America's Ports," September 13, 2004 and Office of the Press Secretary, Department of Homeland Security (2005), "U.S. Department of homeland Security Announces Over $140 million in Grants to Secure Ports," May 13.
[43] Department of Homeland Security, Press Release, "Department of Homeland Security Announces $49 Million in Grants to Secure America's Ports," September 13, 2004.
[44] Department of Homeland Security, FY2005Transit Security Grant Program Allocations, http://www.dhs.gov/interweb/assetlibrary/Grants_FY2005TSGPAllocations_4-12-05.pdf
[45] Bethann Rooney, "Detecting Nuclear Weapons and Radiological Materials: How effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21.
[46] Bethann Rooney, "Detecting Nuclear Weapons and Radiological Materials: How effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21.
[47] GAO report Complete
[48] U.S. Customs and Border Projection, "U.S. Customs and Border Projection FY2006," Monday February 2005.
[49] Department of Homeland Security, Budget in Brief FY2006, p. 16. http://www.dhs.gov/interweb/assetlibrary/Budget_BIB-FY2006.pdf
[50] Caitlin Harrington (2005, "DHS Looking for Cutting Edge Nuclear Devices," Congressional Quarterly, July 29.
[51] Department of Homeland Security (2005), Fact Sheet: Domestic Nuclear Detection Office, April 20. http://www.dhs.gov/dhspublic/display?theme=43&content=4474&print=true
[52] U.S. Customs and Border Projection, "U.S. Customs and Border Projection FY2006," Monday February 2005 and Department of Homeland Security, Budget in Brief FY2006, p. 13.
[53] For a list of ports see http://www.customs.gov/xp/cgov/border_security/international_activities/csi/ports_in_csi.xml
[54] U.S. Customs and Border Projection, "U.S. Customs and Border Projection FY2006," Monday February 2005 and Department of Homeland Security, Budget in Brief FY2006, p. 13.
[55] Ibid, p. 10.
[56] Ibid, p. 20
[57] William Hoehn (2005), "Preliminary Analysis of the US Department of Energy's Fiscal Year 2006 Nonproliferation Budget Request," February.
[58] Amy F. Woolf (2005), "Nonproliferation and Threat Reduction Assistance in Former Soviet Union,"p. 2.
[59] William Hoehn (2005), "Preliminary Analysis of the US State Department's Fiscal Year 2006 Budget Request for Global WMD Threat Reductions Programs," March. See also, Claire Applegarth (2005), "Modest Hikes in Threat Reduction Budget,"Arm Control Today, March.
[60] Ibid.
[61] John Frittelli, "Maritime Security: Background and Issues for Congress," CRS Report for Congress, RL31733, May 27, 2005.
[62] U.S. Customs and Border Projection, *U.S. Customs and Border Projection FY2006*.
[63] Richard Skinner, Office of Inspector General, Department of Homeland Security, "Review of the Port Security Grant Program," OIG-05-10, January 2005. http://www.dhs.gov/interweb/assetlibrary/OIG_05-10_Jan05.pdf
[64] Ibid, p. 4.
[65] Ibid, p. 26.
[66] Ibid, p. 36.
[67] Ibid, pp. 24-25.
[68] Ibid, p. 33.
[69] Ibid, p. 33.
[70] Ibid, p. 34
[71] Ibid, p. 38

[72] Ibid, p. 34.
[73] Ibid, p. 34.
[74] Ibid, p. 26.
[75] Ibid, p. 36.
[76] Ibid, p. 42.
[77] Ibid, p. 17
[78] See Congressional Quarterly. Congressional Transcripts, Congressional Hearings, June 21, 2005, House Homeland Security Subcommittee On Emergency Preparedness, Science And Technology Holds Hearing On Effectiveness Of Nuclear Weapons Detection Technology.
[79] Vayl Oxford, "Detecting Nuclear Weapons and Radiological Materials: How effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21.
[80] Bethann Rooney, "Detecting Nuclear Weapons and Radiological Materials: How effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21.
[81] Congressional Transcripts, Congressional Hearings (2005), House Homeland Security Subcommittee on Emergency Preparedness, Science and Technology Holds Hearing on Effectiveness of Nuclear Weapons Detection Technology, June 21.
[82] Siobhan Gorman and Sydney J. Freedberg Jr. (2005), " Early Warning," National Journal, June 11.
[83] Siobhan Gorman and Sydney J. Freedberg Jr. (2005), p 1745.
[84] Caitlin Harrington (2005, "DHS Looking for Cutting Edge Nuclear Devices," Congressional Quarterly, July 29.
[85] GAO, "Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security, GAO-05-404, June 2005.
[86] Ibid.
[87] GAO, "Container Security: A flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,"GAO-05-557, April 2005, http://www.gao.gov/new.items/d05557.pdf
[88] Permanent Subcommittee on Investigations, "Psi Releases Reports And Findings Detailing Problems With Department Of Homeland Security Programs," May 25, 2005. http://hsgac.senate.gov/index.cfm?Fuseaction=PressReleases.View&PressRelease_id=996&Affiliation=C
[89] Permanent Subcommittee on Investigations, "Psi Releases Reports And Findings Detailing Problems With Department Of Homeland Security Programs," May 25, 2005.
[90] Department of Homeland Security Office of the Inspector general (2005), "Audit of Targeting Oceangoing Cargo Containers: Unclassified Summary," Office of Audits, OIG-05-26, July.
[91] GAO, "Combating Nuclear Smuggling, Effort to Deploy Radiation Detection Equipment in the United States and In Other Countries," Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, GAO-05-840T, June 21.
[92] David Huizenga (2005), "Detecting Nuclear Weapons and Radiological Materials: How effective is Available Technology?" Testimony Before Subcommittee on Emergency Preparedness, Science and Technology The House Committee on Homeland Security, June 21.
[93] GAO, "Combating Nuclear Smuggling, Effort to Deploy Radiation Detection Equipment in the United States and In Other Countries," GAO-05-840T, June 2005.
[94] GAO, "Combating Nuclear Smuggling, Effort to Deploy Radiation Detection Equipment in the United States and In Other Countries," GAO-05-840T, June 2005.
[95] The 9/11 Commission report, "Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, p.381.
[96] The 9/11 Commission report, "Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, p.381.
[97] Author's calculation based on tonnage data from the Army Corps of Engineers (2003 figures): http://www.iwr.usace.army.mil/ndc/wcsc/portton03.htm
[98] Author's calculation based on tonnage data from the Army Corps of Engineers (2003 figures): http://www.iwr.usace.army.mil/ndc/wcsc/stateton03.htm
[99] Office of Inspector General, January 2005, p. 4.

[100] Ibid, p. 17.
[101] Ibid, p. 30
[102] Ibid, p. 27.
[103]
[104] Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March 2003, p. 31.
[105] Mathieu Bunn (2000), "The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material," Carnegie Endowment for International Peace. http://www.ciaonet.org/wps/bum01
[106] Mathieu Bunn (2000), "The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material," Carnegie Endowment for International Peace. http://www.ciaonet.org/wps/bum01
[107] The 9/11 Commission report, "Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition, p.381.
[108] Department of Homeland Security, U.S. Coast Guard, "Statement of Admiral Thomas H. Collins on Homeland Security Missions of the Post 9/11 Coast Guard Before the Committee on Homeland Security, U.S. House of Representatives," June 8, 2005.
[109] Ronald O'Rourke (2005), "Homeland Security: Coast Guard Operations—Background and Issues for Congress," Congressional Research Service, RS21152, June 30, p. 3.
[110] Ibid, p. 3.
[111] Gordon Peterson (2005), "The Coast Guard's Post-9/11 Deepwater Program: An Enduring Solution for U.S. Maritime Security," Domestic Prepardness.com, Volume I, Issue 17, August 24.
[112] Jennifer E. Lake and Blas Nunez-Neto (2005), "Homeland Security Department: FY2006 Appropriations," CRS Report for Congress, RL32863, Updated June 13.
[113] Caitlin Harrington (2005), "New Maritime Security Startegy Imminent," Congressional Quarterly, July 18.
[114] In FY2006 the president requested $1.5 billion for maritime safety, $1.2 billion for maritime mobility and $1.3 billion for maritime environment protection.
[115] For more information about first responder grants see Veronique de Rugy (2005), "What Does Homeland Security Money buys?", AEI.
[116] Matthew Bunn, Anthony Wier, and John P. Holdren (2003), "Controlling Warheads and Materials: A Report Card and Action Plan," The Nuclear Threat Initiative, March.
[117] Charles D. Ferguson II and William C. Potter (2004), "Terror and Nuclear Threat," San Jose Mercury News, October 10.
[118] Wier, Hoeln and Bunn (2004), "Threat Reduction Funding in the Bush Administration: Claims and Counterclaims in the First Presidential Debate," October 6.
[119] Randall Scasny (2005), "Congress Unhappy with Coast Guard Modernization Plan," Coast Guard News, July 29.
[120] Author's calculation based on the Budget of the United States, FY2006, the Department of Homeland Security, *Budget in Brief FY2006*, and U.S. Customs and Border Projection, *U.S. Customs and Border Projection FY2006*.