

Center for American Progress



New Strategies to Protect America: Safer Ports for a More Secure Economy

by Joseph F. Bouchard, Ph.D.



HOMELAND SECURITY

Critical Infrastructure Strategy Series

CRITICAL INFRASTRUCTURE SECURITY SERIES

New Strategies to Protect America: Safer Ports for a More Secure Economy

EXECUTIVE SUMMARY

A review of security measures and policies at commercial ports in the United States reveals significant deficiencies despite changes mandated under law. The Bush Administration has failed to set priorities based on the risks posed to our economy and society and it now proposes to eliminate the grants program that supports the implementation of port security plans. Adopting a risk-based approach – differentiating between sites and determining which ports are most in need of protection – can achieve greater security at a lower cost. Continuing on our current path carries with it the risk of grave consequences to our society and economy

The Maritime Transportation Security Act (MTSA) was signed into law in the wake of the September 11, 2001 al Qaeda attacks on the United States. The deadline for implementing MTSA was July 1, 2004. Unlike other areas of critical infrastructure security, where the Bush administration has been unwilling to set clear mandates for the private sector and push for meaningful change, the MTSA has been a catalyst for action. Unfortunately, in the face of unrealistic deadlines and disjointed implementation milestones, action on paper has not necessarily translated into greater security at the pier. The priorities established for maritime transportation security plans wrongly assume that all ports, facilities and vessels are equally vulnerable to attack and that all need to be protected to the same security standard. A risk-based approach that takes into account the actual terrorist threat that we face, and concentrates on risks that carry the gravest consequences to our society and economy, can actually achieve more security at potentially lower cost.

The United States is a maritime nation. We rely upon and profit from global commerce worth trillions of dollars. Any major disruption of these worldwide supply chains will instantly create billions of dollars in economic loss and create cascading effects in every corner of the world. Against this backdrop of risk, the Bush administration and its Department of Homeland Security have failed to dedicate sufficient resources to adequately protect the maritime transportation system that is vital to our society, economy and way of life. Port security is currently an unfunded mandate and that situation will deteriorate because the

Bush administration plans to eliminate the specific grant program – poorly funded as it is – that supports municipal, state and private sector owners and operators as they attempt to implement security plans required by the MTSA.

The Center for American Progress proposes a four-point strategy that will lead to safer ports and make our people and economy more secure. The optimum strategy for protecting maritime transportation requires a risk-based approach to integrating security, consequence reduction, and emergency preparedness and continuity of business into comprehensive plans and programs for enhancing the resilience of the maritime transportation system. Its major features include:

- Revising Coast Guard maritime facility security regulations and, if necessary, amending MTSA to emphasize risk assessments focused on the threat and consequences of a terrorist attack rather than vulnerability;
- Increasing attention to risk mitigation, preparedness and continuity of operations to enable the maritime transportation security system to recover quickly in the event of a terrorist attack, reducing the economic consequences of a severe disruption, thereby denying attackers their central strategic goal;
- Maintaining the existing Port Security Grant Program, creating greater program flexibility for an improved return on investment and increasing annual funding to a minimum of \$500 million per year in order to eliminate the current mismatch between strategy and resources and make port security a funded federal mandate; and
- Establishing a national port security trust fund by dedicating a specific percentage of customs revenue collected on goods flowing through our nation’s ports in order to ensure long-term sustainability of our maritime transportation system security.

This report focuses on security measures at or near U.S. shores. It is limited in scope to policies and issues directly related to MTSA implementation and its impact on the 361 commercial ports in the United States; roughly 3,700 maritime facilities, including cargo and passenger terminals, in those ports; and approximately 60,000 ships that arrive in U.S. ports annually, including about 8,100 foreign flag vessels. Although cargo, container and supply chain security are mentioned in MTSA, these very important issues will only be tangentially covered. Port security also encompasses what is termed “maritime domain awareness,” which includes security on the high seas and abroad. The emphasis is on the Department of Homeland Security (DHS) and the agencies within it,

particularly the U.S. Coast Guard, not other federal departments and agencies that play important but supporting roles.

President Bush repeatedly stresses that America must “stay on the offensive” against terrorism. However, overseas military operations alone cannot protect the United States from the threat of terrorism. The question is whether enough is being done now to make our homeland more secure. The answer is no.

MARITIME TRANSPORTATION SECURITY BEFORE MTTSA

Prior to September 11, 2001, the maritime and port industry maintained a relatively low baseline of security, particularly relative to other surface transportation sectors, most notably the airline industry. From a port security standpoint, the primary focus was theft, not terrorism. To the extent that smuggling was a concern, it was drugs, not weapons of mass destruction. This was not due to negligence on the part of state port authorities and private sector facility operators; it was the result of rational business decisions that accurately reflected their security concerns.

The maritime and port industry only made modest security efforts because the shift from break bulk shipping (large quantities of goods that are on-loaded and off-loaded in lots) to containerization had greatly reduced theft and, like many businesses, a small amount of loss was viewed as a cost of doing business. This was compounded by the overwhelming emphasis on efficiency and cost reduction in the international shipping system. The shipping industry is highly competitive, making investments in security difficult to justify when losses to criminal activity are exceptionally low.

The federal government implicitly endorsed this low priority; it had not imposed security standards on the maritime industry and, in fact, had no overarching maritime or port security program of its own. Unlike airports and airlines, which began implementing security measures in the 1960s due to a wave of skyjackings, the U.S. maritime industry had not experienced dramatic security incidents that prompted political pressure for enhanced security measures. Other than efforts by Customs and the Coast Guard, supported by other Federal agencies, to keep illegal drugs out of the country, the only mandated port security program in effect on September 11 was based on the 1950 Magnusson Act. That act gave the Federal government authority to control access to U.S. ports by merchant vessels of the Soviet bloc and other hostile nations. However, with the demise of the Soviet Union, its enforcement emphasis shifted to preventing espionage, smuggling or other illegal pursuits by any nation hostile to the United States. Although the Coast Guard was still assiduously enforcing the Magnusson Act in 2001, its impact was limited because potentially

threatening vessels were identified only on the basis of their flag of registry – widely recognized as almost meaningless in an era in which the vast majority of vessels were registered in “flag of convenience” nations.

What national policy attention port security did receive prior to September 11 was attributable to two factors that emerged during the 1980s. First, the 1985 hijacking of the Italian cruise ship *Achille Lauro* prompted increased efforts to prevent terrorists from easily gaining access to cruise ships.¹ Second, the rise of the South American drug cartels and their incessant efforts to find innovative methods of smuggling illegal drugs into the United States – and drug money and other illicit goods out of the country – had prompted growing concern for port and cargo security as it became apparent that the international shipping system provided a lucrative channel for smuggling.²

Senator Bob Graham (D-FL), concerned about the disproportionate impact that drug-related crime was having on Florida’s ports, was an early leader in the effort to enhance the security of America’s ports and in the late 1990s began working on legislation to address the issue. Senator Graham’s concerns found a sympathetic ear at the White House, which was pursuing a wide range of efforts to better protect the United States against terrorism. President Clinton on April 27, 1999 signed an Executive Memorandum establishing the Interagency Commission on Crime and Security in U.S. Seaports, which published a report of its findings and recommendations in the fall of 2000. This important report accurately identified the serious vulnerabilities of U.S. seaports to terrorism and criminal activity, and recommended a wide range of measures for mitigating those vulnerabilities.³

Although the report of the Interagency Commission received little attention in the press, senators and representatives from states with major seaports pushed for further port security enhancements. On July 20, 2001, Senator Ernest F. Hollings (D-SC) and 14 co-sponsors (Senator Graham prominent among them) introduced S.1214, originally referred to as The Port and Maritime Security Act of 2001. The bill originally was focused on crime, cargo theft and smuggling in America’s seaports, but was significantly revised and expanded after being reported out of committee on August 2, 2001 to more fully address the terrorism threat. The final bill was signed into law by President Bush on November 25, 2002.⁴

THE ECONOMIC STAKES

Increased emphasis on port security is certainly warranted by the critical and growing importance of maritime transportation to the U.S. economy.

Consider that:

- About 95% of U.S. imports by weight and 80% by dollar value enter the United States by sea. That's 2.4 billion tons of goods valued at more than \$1 trillion. Sea borne trade is expected to double over next 20 years.
- About 4 billion barrels of oil per year – 62% of U.S. consumption – are imported by sea.
- About 90% of the manufactured goods imported into the United States from overseas each year arrive in shipping containers.
- About 9 million shipping containers enter the nation via its seaports each year.
- A total of about 200 million shipping containers are in use worldwide.
- Customs duties collected on goods entering the United States via seaports average \$15.2 billion a year.

As these figures also show, maritime transportation is a daunting challenge.⁵ We live in an era of “just in time delivery” that greatly increases the importance of protecting maritime transportation from disruption. Factories, wholesalers and retailers no longer maintain large inventories in warehouses due to the cost of storing them and the emphasis on agility –the shipping system itself acts as virtual warehousing. Inventories that used to sit in warehouses are now in shipping containers en route to the customer. Just in time delivery has helped increase productivity and profitability for many U.S. companies and has reduced the cost of the goods consumers purchase, but it has increased the vulnerability of the U.S. economy to disruption of international trade or maritime transportation.

Various estimates have been made of the impact that a terrorist attack on a seaport would have, particularly if the federal response were to shut down all shipping. On September 11, all air, land and sea ports of entry were closed. This caused some factories to shut down and stores to run low on some goods.⁶ The 2002 dock worker lockout at the ports of Los Angeles and Long Beach is estimated to have cost between \$6.3 billion to \$19.4 billion in loss to the U.S. economy, with the lower figure being most credible. A 2002 port security war game, which simulated a nine-day shutdown of all U.S. ports, resulted in an estimated \$58 billion loss. The Brookings Institution estimated that a successful terrorist attack with a weapon of mass destruction smuggled into the country in a shipping container could amount to \$1 trillion if subsequent draconian security

measures were adopted that impeded trade.⁷ A Center for Homeland Security and Defense (CHSD) estimate of the impact of a terrorist attack on U.S. ports begins with an immediate impact of between \$1.5 and \$2.7 billion dollars a day loss; rising to \$5 billion a day after 3-5 days; and exponentially within 10-15 days. After about 45 days, perhaps even sooner, the U.S. economy would collapse into an unprecedented depression due to a severe energy crisis, widespread shortages and rampant price gouging by the energy industry.⁸

While estimates of the economic cost of a terrorist attack on the maritime transportation system vary depending on the many variables involved and assumptions used, the stakes are clearly enormous.

MTSA IMPLEMENTATION

MTSA did not articulate a strategy *per se*, but did state that “[i]t is in the best interests of the United States” to ensure the free flow of commerce and efficient movement of cargo, improve communications among law enforcement officials responsible for port security, establish requirements for security programs and physical security at port facilities, provide financial assistance to the states and private sector to increase physical security of U.S. ports, develop technology for non-intrusive detection of crime at U.S. ports, and enhance cargo security through increased intelligence collection on intermodal transportation and private sector in-transit visibility of cargo that can support law enforcement efforts to manage security risks.⁹ Key MTSA provisions called for the development of:

- Vulnerability assessments of facilities and vessels;
- National, area, facility and vessel security plans, and facility and vessel incident response plans;
- Transportation security cards, since named the Transportation Worker Identification Credential (TWIC);
- A maritime security grant program;
- A number of Coast Guard-managed programs, including maritime safety and security teams, maritime security advisory committees, security assessments of foreign ports, and a vessel automatic identification system; and
- A program to enhance cargo and intermodal transportation security.

To implement MTSA the U.S. Coast Guard published extensive and detailed maritime security regulations.¹⁰ However, a compressed and disjointed timeline for implementing the act has definitely affected what the MTSA has actually accomplished in its first year. It remains to be seen whether or not the thousands of facility security plans, scores of area plans and an overarching

national plan collectively have achieved unity of purpose and coherent operational procedures for preventing attacks on the maritime transportation system. These plans alone collectively fall far short of the goals set by MTSA. Overall, too many facility plans are little more than lists of activities that individually and collectively fall far short of the goals set by MTSA. For example:

- While the Bush Administration has repeatedly asserted that implementation of MTSA has been an unqualified success story, individual facility security plans were written before broader area maritime security plans were accomplished, creating a kind of “cart and horse” problem that remains to be resolved.
- While the Coast Guard began formulating new regulations in January 2003,¹¹ it did not issue final regulations until October 22 – barely two months before the MTSA-mandated December 31, 2003 deadline for facilities and vessels to submit their security plans. Although most facilities began their efforts to comply with MTSA before the final regulations were published – they had no choice – major investment decisions were deferred pending decisions on facility security plans.
- Some facilities were forced to submit plans they knew would be inadequate and would not be approved by the Coast Guard merely to avoid being sanctioned for missing an unreasonable deadline – a tactic that bought them up to six more months to get their plans right.
- Facility security plans, which in many cases were not approved until March 2004 or even later, left operators very little time to take action. To make matters worse, the Coast Guard published revised implementation guidance on May 27, 2004, only one month before facilities were ostensibly required to complete MTSA security plan implementation.¹²

Of course, this confusion didn’t prevent the Bush administration from touting its maritime security efforts as a complete success. On June 21, 2004, a week before the deadline for MTSA implementation, Homeland Security Secretary Tom Ridge stated in a speech at the Port of Los Angeles, “I am pleased to announce that as of today, the United States is in full compliance with the requirements of the International Ship and Port Facility Security Code [ISPS] – just in time to meet the July 1st deadline. ...The Coast Guard has received nearly one hundred percent of the security assessments and plans required under this law [MTSA]. When the deadline arrives, ports and vessels will have already begun implementing these new security measures around the country.”¹³

However, this rosy picture confuses activity with accomplishment. Grand plans on paper have not been translated into meaningful security at the pier. Serious problems still remain to be solved.

MISMATCH OF STRATEGY AND RESOURCES

While the federal government publicly espouses many priorities, to find out just how important a program is, as the expression goes, “show me the money.” The budget is a concrete expression of the priorities of, in this case, the Department of Homeland Security. Judging from the Port Security Grant Program, despite the obvious importance of ports to the U.S. economy, it is not very high. There are three serious problems: first, the level of funding for port security grants is inadequate to implement MTSA; second, while DHS is beginning to employ a risk-based approach, it is not being applied properly; and third, the program lacks sufficient flexibility to enable recipients to invest funds where the security return on investment will be greatest. The Bush administration’s solution to these problems is to actually eliminate the program altogether, which will only make a bad situation much worse.

The MTSA states that the purpose of the Port Security Grant Program is “...a fair and equitable allocation among port authorities, facility operators, and state and local agencies required to provide security services of funds to implement Area Maritime Transportation Security Plans and facility security plans.”¹⁴ MTSA did not define “fair and equitable,” nor did it suggest a specific funding level or formula. However, the act did list the eligible costs that could be defrayed under the Port Security Grant Program: additional security personnel required to comply with the Coast Guard regulations, acquisition, operation and maintenance of security equipment or facilities, screening equipment, and vulnerability assessments.¹⁵ Absent a definition in MTSA, a reasonable funding approach would make port and facility operators eligible for grants to cover compliance with the Coast Guard facility security regulations above the costs that the organization would have incurred in the course of implementing industry standards of best practices for facility security. In other words, facilities are responsible for their own security to the level defined by standard maritime transportation industry risk management practices, while the Federal government should fund all additional security costs incurred in enhancing homeland security. Unfortunately, the Bush Administration eschewed a fair and equitable allocation of funds and instead imposed an unfunded mandate on the maritime transportation industry.

The Coast Guard estimates that it will cost \$7.3 billion for the U.S. maritime industry to implement MTSA, including initial costs and annual costs through 2013, with the split among vessel, facility and port security.¹⁶ To accomplish this, the American Association of Port Authorities estimates that a minimum of \$400 million per year is required.¹⁷ Yet, actual funding to date has only averaged \$115.5 million between fiscal years 2002 and 2006. To put that in context, even if current levels are maintained, full MTSA implementation will take 47 years. Given these current funding levels, the United States will land an astronaut on Mars as much as 95 years before it completes implementation of MTSA.¹⁸ This is very good news for terrorists, but not for our security.

Through 2004, there is roughly a \$1.5 billion gap between what the capital investment that public and private port security operators say is required for MTSA implementation and what the federal government has been willing to support. This is exacerbated by the fact that the Bush administration expects state governments, via their port authorities, and the private sector to pick up the vast majority of the bill – as much as 93 percent of the total – in personnel and operating costs associated with MTSA implementation. But as the accompanying table shows, in every round of the Port Security Grant Program to date, requirements have far out-stripped available resources. This is not the way a successful “partnership” functions.

Grant Round	Total Grant Proposals	Grant Funds Available	Port Security Gap
Round 1 (June 2002)	\$695 million	\$92 million	\$603 million
Round 2 (June 2003)	\$997 million	\$245 million	\$752 million
Round 3 (December 2003)	\$987 million	\$179 million	\$808 million
Round 4 (September 2004)	\$643 million	\$50 million	\$593 million

Table 1. Port Security Grant Funding vs. Grant Proposals, 2002-2004¹⁹

The Bush administration’s presumption that state port authorities and the private sector have the resources at hand to fully implement the MTSA is suspect. Among major ports, only Los Angeles and Long Beach actually make a profit. Most ports rely directly or indirectly on a subsidy. States are willing to do this because the taxes they collect from the commercial maritime industry that use their ports exceed the cost of the subsidy to the port authorities. The specific source of that state funding varies from state to state, but in every case the port authority competes with other state agencies and programs for funds. However, states and municipalities, unlike the federal government, cannot run budget deficits of their own and have to rationalize competing budget demands regarding education, health care and security (including unplanned personnel costs associated with the ill-fated color-coded alert system or other emergencies). The private sector operates on low margins in a competitive environment.

Security investments are part of any company's overhead, which successful companies are relentlessly trying to reduce through increased productivity and outsourcing. There are definitely synergies between greater efficiency and improved security, which smart upfront investments can achieve. While there is no doubt that private sector operators will be required to contribute significantly to port security, the most effective approach is to combine strong mandates with incentives such as grants that serve as catalysts for change. Without the incentives, the pace of change will be slower – a problem when faced with the on-going threat of a terrorist attack.

There is also a fundamental issue of fairness. MTSA was enacted to protect the entire nation against terrorism, not just its ports. The Bush Administration policy of transferring the tax burden for port security from the Federal government down to the states means that port states are subsidizing security for non-port states. Every major port already faces a huge requirement for investment in port growth and productivity, an investment that comes from the states – usually in the form of bonds for port development. The best option going forward is for states and the private sector to make security integral to the design and construction of future port facilities. The federal government should be willing to contribute to such an investment. Otherwise, funds will not be available for expansion of port capacity and productivity to handle expected growth in maritime trade – which strengthens our economic security and ultimately our national security.²⁰

The Port Security Grant Program also has suffered from serious management issues, particularly relating to grant allocation decisions based on politics and not on risk. The Transportation Security Administration, which managed the program before the advent of DHS, attempted to implement a rational review and allocation process that included local and headquarters-level review of applications by subject matter experts from the Coast Guard and Maritime Administration, although the results were disappointing.²¹ Bowing to Congressional pressure, when it took over, DHS distributed port security grants as widely as possible, in some cases for projects of dubious value with little regard to the risk or consequence of a terrorist attack.

Only this year has the department made an initial effort to implement a “risk-based” approach in the current fiscal year 2005 (Round 5) program. This effort to articulate risk-based priorities is laudable, but is seriously flawed. Because of limited funds, only 66 of our largest ports are eligible for grants, with emphasis placed on prevention and detection of improvised explosive devices, particularly those delivered by small craft, underwater or in vehicles on ferries.²² Prioritizing entire ports for grant allocations misses the important point that not all facilities within a port present the same level of risk: some may be seriously threatened because an attack on them would cause catastrophic

consequences, while other facilities in the same port would be of little interest to terrorists. Although DHS recognizes that “the highest risk assets include oil, chemical, gas terminals and passenger/ferry vessels/terminals,”²³ this was not incorporated into this year’s grant prioritization process. Thus, a low-risk facility at a high-risk port can apply for a port security grant, while a high-risk facility in an otherwise low-risk port cannot. The failure to distinguish priorities within rather than between ports means that the allocation of scarce port security grant funds will not accrue the greatest return on investment, leaving significant and exploitable security gaps at U.S. ports.

In this current grant round, DHS plans to require 50 percent cost sharing to the private sector, but only 10 percent to public agency applications, a criteria based on politics rather than risk. This suggests that securing a publicly owned facility of no interest to terrorists will receive grant support, but a privately-owned LNG storage tank that places thousands of people at risk will not.

Existing grants come with inherent limitations that both inhibit MTSA implementation and call into question whether security improvements that are being made can be sustained over time. Grants can only be used to purchase and install security equipment and systems, and not to pay salaries, maintenance and other operational costs, which make up the bulk of the cost of implementing MTSA.²⁴ This means that, of the \$5.4 billion that the Coast Guard estimated will be required for enhanced facility security through 2013, about \$4.9 billion cannot be funded with port security grants under the current rules.²⁵ This poses two problems for genuine compliance with the MTSA. Not only will security improve at a slower rate, as security maintenance costs increase over time as equipment ages, existing restrictions will force port authorities and private facilities to resort to the wasteful practice of applying for grants to replace equipment before the end of its expected service life – not because it is necessary but because it is the only available route to grant support.

The grant program is at risk of disappearing altogether even as requirements for port security expand.²⁶ In its fiscal year 2006 budget request, the Bush administration proposed to abolish the Port Security Grant Program and replace it with a Targeted Infrastructure Protection (TIP) grant program covering all surface transportation and other critical infrastructures, such as chemical plants and energy facilities. The Bush Administration requested a mere \$600 million for the Targeted Infrastructure Protection grant program in fiscal year 2006. TIP grants would be allocated via the states.²⁷

In its February 2005 Interim National Infrastructure Protection Plan, the Department of Homeland Security listed 17 critical infrastructure sectors. With the exception of banking and finance, none of the other areas, which include

agriculture, public health, telecommunications and information technology, are as vital to the American economy as transportation systems and maritime transportation more specifically. As we have already seen in recent years, distributing grants through states rather than directly to grant applicants slows the process down and leaves it vulnerable to politization. Competition within critical infrastructure sectors can lead to efficiencies and the development of best practices over time. Competition between critical infrastructure sectors guarantees that scarce resources will be spread too thin. It is ironic that eight months after implementation of federal statutorily mandated regulatory requirements for port security – where ports, facilities and vessels can be fined or shut down by the Coast Guard for failing to comply with MTSA security regulations – the Bush administration and Department of Homeland Security have eliminated (rather than expanded) the tailored federal grant program that is critical to the success of MTSA implementation.

A straightforward solution to guarantee adequate long-term funding stream for MTSA implementation and port security sustainability would be to earmark a small portion of the \$15.2 billion in customs revenues collected on goods moving through the nation's ports each year and establish a national port security trust fund.²⁸ Adequate funding could be achieved by designating as little as 3% of those customs duties, achieving the MTSA goal of a “fair and equitable” allocation of funds for implementation.

A RISK-ORIENTED PORT SECURITY STRATEGY

Maritime transportation security demands a fundamental rethinking of our approach. A viable strategy must be based on a realistic risk assessment and understanding of what can port authorities and the private sector reasonably can be expected to accomplish, rather than cynical imposition of an unfunded mandate cloaked in hollow euphemisms about “partnership.” Maritime transportation security needs to move in new directions in three areas:

- Base security requirements on assessments of risk – what the threat actually is and what the consequence of an attack would be;
- Increase the emphasis on risk mitigation, preparedness and continuity of operations;
- Expand the Port Security Grant Program to speed MTSA implementation and commit sufficient resources to ensure long-term port security sustainability.

Risk-based Security Requirements

The current approach to maritime transportation security mandated by MTSA and the Coast Guard maritime security regulations establish a single, universal set of security standards and requirements for all port facilities, regardless of size, type, likelihood of being attacked or potential consequences of an attack. This approach evolved out the MTSA narrow focus on vulnerability assessments as the basis for security planning.²⁹ Although the Coast Guard maritime security regulations acknowledge that certain port facilities, such as cruise ship passenger terminals, have unique security requirements, overall the approach is universal compliance with a stringent, inflexible set of requirements. For example, a pier for loading or unloading cement must both implement the same measures as a liquefied natural gas (LNG) terminal.

The implicit assumption underlying the current vulnerability-based approach is that each and every port facility is equally likely to be attacked by terrorists and would generate the same consequences in terms of loss of life and loss to the American economy. This, of course, is nonsensical and demonstrates a disturbing lack of understanding of the threat posed by global extremist terrorist groups like al Qaeda. All facilities are vulnerable to some degree and there is no end to the wildly imaginative threat scenarios that can be generated to justify channeling scarce funds in one direction or another. This is the essence of the political tension within Congressional oversight committees over funding for urban vs. rural states, for example. All states are theoretically at risk, but terrorism risk does not apply to all states equally. Without such a strategic approach based on the actual threat and the likely consequence of a terrorist attack, strenuous efforts and extravagant expenditures will end up contributing little to enhancing maritime transportation and more broadly our national security.

A flexible system of risk-based security requirements would achieve greater enhancement of overall homeland security at less cost than the current approach. What is needed is a methodology for integrating threat, consequences and vulnerability into a comprehensive risk assessment and a provision allowing facilities to tailor their security plans to their specific level of risk.³⁰

Threat analysis. Not all port facilities are equally likely to be terrorist targets. The United States faces sophisticated terrorist networks that want to attack us politically and economically. They are interested in strikes that are visible and symbolic, yet also kill large numbers of people; that meaningfully disrupt our economic and social systems; and that they can exploit to fan anti-Americanism and discontent around the world. Contrary to our current approach, such an attack is not likely to be random. Jihadist groups like al Qaeda

don't operate that way. Knowing this, the information we have on terrorist threats should be used to prioritize types of facilities and require those more likely to be attacked to meet higher standards than those less likely to be attacked. Examples of high priority targets: petroleum terminals. Examples of low priority targets: coal terminals, break bulk terminals and auto terminals. Container terminals themselves are not likely targets for external attack; exploiting containers so as to shut down global supply chains is a far more likely scenario.

Threat analysis needs to clearly distinguish between a facility being a target of terrorist attack and a facility being a conduit for smuggling. Current policy implicitly assumes that all facilities of any type are equally likely to be used as a conduit for smuggling, as well as being equally likely to be attacked. This is not the case. Port facilities that are more prone to smuggling, such as the intermodal facilities that handle shipping containers, should have stronger measures to prevent terrorists from circumventing U.S. Customs and Border Protection (CBP) detection efforts. Conversely, most intermodal port facilities are not a lucrative target for attack and minimum security measures described above will suffice to protect them from attack.

Consequence analysis. Because we have only fragmentary and ambiguous intelligence on the activities of terrorist groups, prudence demands that we supplement the threat analysis with an analysis of the consequences if different types of port facilities are attacked. In other words, think like a terrorist. There are two elements of consequence analysis: mass casualties and economic loss.

Knowing that terrorist groups like al Qaeda want to cause mass casualties, port facilities near urban centers that would provide terrorists an opportunity to cause mass casualties should meet higher security standards. Examples of such targets: LNG and LPG terminals, other bulk hazardous materials terminals, and cruise ship passenger terminals. Also, since economic loss is a terrorist objective, we have to protect potential targets of importance to the U.S. economy. It is not clear how sophisticated they are at analyzing the economic impact of attacking specific targets, but in many cases, the information needed to identify a lucrative target is readily available on-line.

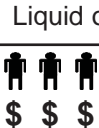



DHS can choose from a number of tools for integrating threat, consequences and vulnerability to produce a risk assessment. Four methodological best practices should be incorporated:

- Use quantitative data as much as possible, particularly for measuring consequences and vulnerability;

- Where subjective judgments must be applied, employ a panel of impartial subject matter experts to minimize the impact of personal biases and provide a broad range of expertise. The insurance industry, quite familiar with risk management and mitigation strategies, already employs this approach;
- Establish clearly documented assessment and factor weighting criteria that allow risk assessments to be audited, thus ensuring the credibility of outcomes; and
- Put in place procedures to review and validate the data used in the risk assessment (including accuracy and credibility of sources), the analytical process itself (via review by outside experts in this type of analysis), and the outcomes (via a “red cell” or other body that thinks like an adversary and does a parallel assessment of weaknesses and potential scenarios).

Security requirements matrix. Risk-based security requirements would categorize facilities based on a two-dimensional assessment that combines the level of risk based on an assessment of threat, consequences and vulnerability with the type of facility, including whether hazardous materials are present. Discrimination could be as simple as just two levels (high or low risk) or include more gradations.

The result is a matrix in which each cell would contain security requirements tailored to the type of facility and level of risk, as shown in the illustrative matrix at Figure 1. For simplicity of illustration, the risk categories in Figure 1 are ranked on the basis of consequences; the actual methodology incorporates threat and vulnerability as well. The actual risk levels and facility categories would be derived from a thorough analysis to identify the optimum number of cells for establishing risk-based security requirements. Each cell would contain security requirements tailored to the unique circumstances of facilities at a particular risk level and of a particular type.

Risk	Container Terminal	Passenger Terminal	Non-Hazardous Bulk Terminal	Hazardous Bulk Liquid or Gas
Mass Casualties High Economic				
Mass Casualties Low Economic				
Low Casualties High Economic				
Low Casualties Low Economic				
Security Requirements Matrix				

All facilities, even those with lowest risk, would have to meet universal minimum physical standards, such as controlled access. This is already envisioned through the proposed Transportation Worker Identification Credential (TWIC). Beyond that, security requirements would be facility-specific based on the level and type of risk it represents. Security requirements for that facility and its eligibility and priority for port security grants would be commensurate with its risk assessment. For example, smaller facilities (those less likely to be attacked and those that would not result in catastrophic loss if attacked) would have less stringent – and less costly – security requirements. For container terminals, the emphasis would be on security measures that prevent operatives or contraband, particularly weapons of mass destruction, from entering the country. Port facilities that handle large quantities of explosive or hazardous materials, such as LNG, petroleum and chemical terminals, would focus on measures to prevent terrorists from gaining access to the terminals with improvised explosive devices in order to cause catastrophic damage to storage and piping systems.

Unlike the current approach to maritime security, risk-based security requirements would be affordable, allowing limited resources to be spent on measures providing the greatest return on investment. Also, from a business perspective, homeland security measures would more closely align with the business interest in theft prevention, and managing potential liability and insurance costs. This risk-based approach would suppress the tendency to exaggerate vulnerability assessments in order to attract funding for expensive and unnecessary security systems – the epitome of low return on investment. For most facilities, meeting risk-based security requirements would result in emphasis on physical security (fences, gates and barriers), perimeter surveillance, and access control – all of which could be very simple yet more than adequate for a low-risk facility. High-risk facilities, on the other hand, would have to meet more stringent security requirements, probably would require more extensive and sophisticated security and monitoring systems, and thus would have high priority for port security grants.

Continuity of Operations, Risk Mitigation and Preparedness

On September 11, the United States temporarily shut down all air traffic; closed land borders and halted maritime shipping into the country in response to the four terrorist hijackings. The response was understandable in light of the uncertainty of what we confronted. However, while warranted, our response had greater negative impact on the U.S. economy than the attack itself.

It has taken more than three years for U.S. policy to move beyond the approach taken on September 11. Senior U.S. officials and homeland security analysts made a number of alarmist comments over the past three years that a

single attack on a port or discovery of a single weapon of mass destruction in a shipping container would force closure of all ports and shutdown of the entire intermodal transportation system until DHS and FBI could assess the potential for further incidents. Obviously, such an approach actually provides terrorists a strong incentive to attack a U.S. port. At best, a total shutdown delays, but does not ultimately thwart further attacks.

With the promulgation of Homeland Security Presidential Directive 13 (HSPD-13), “Maritime Security Policy” in December 2004, U.S. policy is beginning to evolve in a more constructive direction. HSPD-13 identified expedited recovery and response in the maritime domain as one of six core elements of U.S. policy, and “critical to the economic well-being of our Nation.” It tasked the Secretary of Homeland Security to set “comprehensive national maritime infrastructure recovery standards” and develop a Maritime Infrastructure Recovery Plan (MIRP) no later than June 21, 2005.³¹ The draft MIRP is in interagency circulation for review and comment. It defines federal, state, local and private sector roles and responsibilities, and outlines a concept of operations for maritime recovery based on the National Response Plan and National Incident Management System. HSPD-13 and the MIRP are an improvement, but fail to address major issues related to security and continuity of operations of the maritime transportation system. The fundamental problem with the HSPD-13 approach, which is likely to be central to the MIRP, is the distinction drawn between security and recovery: the two are treated as independent, if not mutually exclusive, policies and objectives.³² The right approach is to fully integrate security and recovery into a unified concept emphasizing continuity of operations in the maritime transportation system.

U.S. policy should emphasize isolating the impact of a terrorist attack on the maritime transportation system, using all available sources of information to determine if it is a stand-alone incident or one of multiple attacks, and implementing selective measures focused on countering specific threats. An analogy to the airline industry is appropriate. After a commercial airplane crash, the National Transportation Safety Board attempts to make a rapid assessment of whether the causes were isolated factors or broader systemic or structural failures. It has the option to ground specific types of aircraft for further inspection while allowing the broader commercial aviation system to continue to function. Likewise, the maritime transportation system has to develop a similar ability in the event of an incident to identify and isolate the components that failed without shutting down the entire intermodal transportation system. This can only occur if security (backed by improved surveillance, information collection and analysis capabilities) becomes an integral part of doing business. Certainly, information technology that already enables anyone to track shipments anywhere in the world should offer opportunities for enhanced security.

Additionally, procedures for rapidly shifting cargo and passenger flows from terminals or routes that have been disrupted or are likely to be threatened would greatly reduce the impact of protective responses.

Continuity of operations. The RAND Corporation published a study in 2004 on supply chain security that emphasized the importance of the “fault tolerance and resilience” within the international shipping system – its ability to rapidly adapt to and compensate for disruption of a major shipping route.³³ This is a valuable concept for integrating security and recovery into a broad approach for maintaining continuity of operations in the maritime transportation system.

To a large degree the shipping system is self-synchronizing and shippers will immediately begin making plans to divert vessels and cargo to other ports in the event of a terrorist incident disrupting maritime transportation through a port. The federal government should not attempt to directly control this process; it has neither the knowledge nor the resources to do so effectively. However, only the federal government is in a position to inform the private sector of existing port restrictions so that any diversion of shipping and cargo following a terrorist attack will work; and require reports from the private sector and port authorities on ship diversion plans so that federal resources in those ports, especially the Coast Guard and U.S. Customs and Border Protection (CBP) are available to support those plans. The Coast Guard Captains of the Port and CBP Port Directors will play critical roles, rapidly identifying personnel and equipment needs at ports that remain open and accessible. The Coast Guard would need to shift personnel and small craft to increase their capacity to conduct ship boardings, inspections and elevated harbor security. CBP probably would need to shift agents and inspection equipment (Gamma and X-ray scanners and radiation detection equipment) to increase its capacity for container and cargo inspections, and immigration control, particularly if passenger vessels must be diverted. The development of a standard methodology for such resource assessments and a national “triage” system for reallocating Coast Guard, CBP and other DHS resources among multiple ports in order to keep ports open and our economy functioning must be a priority.

The key is effective coordination and communication among port authorities, private facility operators, private sector importers and exporters, and federal, state and local agencies. Real-time information is required across all 50 states because maritime diversions will impact truck and rail traffic volume. State governments can advise the transportation system about highway construction and other impediments that could create bottlenecks. In extreme circumstances, where key ports have been severely damaged and diversions are likely to be lengthy, the U.S. Department of Transportation may even need to reprogram highway construction funds to rapidly complete a project urgently needed to

minimize disruption of cargo flow. Unfortunately, the transportation bill currently in conference does not include any major surface transportation security provisions.

Risk mitigation. While deterrence may not work against an individual terrorist determined to die, plots against specific targets may be deterred by reducing the risk of mass casualties or grave economic loss. For many high-risk port facilities, we achieve a greater return on investment from risk mitigation than from enhanced security measures. Even if an attack does occur, the response will likely be easier and the recovery more rapid.

Risk mitigation focuses on safety, reliability and disaster prevention measures already covered in laws and regulations addressing safety and environmental protection. In other words, the Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA) have an important role to play in U.S. homeland security efforts. For example, double-hull tankers are required to reduce the likelihood of an oil spill in an accident, but they can also reduce the likelihood of an oil spill as a result of a terrorist attack. Similarly, oil pollution prevention and response regulations enforced by EPA and the Coast Guard contribute to reducing the consequences of a terrorist attack on a waterfront petrochemical terminal. The weakness in current laws and policies is that they are designed to prevent or mitigate the consequences of accidents or natural disasters and in many cases may not be adequate for the magnitude of damage that can be caused by a terrorist attack.

Risk mitigation strategies have been common in the private sector for some time, particularly with respect to liability and insurance coverage. There are synergies between security and risk mitigation that can make both more effective. For example, relatively modest investments in redundant quick closing valves or berms that contain spillage from oil storage tanks would offer a greater return on investment than very expensive security systems of dubious value for preventing a terrorist attack.

Consequence reduction measures may allow security efforts to be focused on defenses against specific types of attacks rather than every conceivable type of attack, or to focus on protecting particularly vulnerable points in a facility rather than the entire facility. Conversely, security measures can reduce the effectiveness of an attack, enhancing the performance of consequence reduction measures. Increasing the complexity and reducing the impact of an attack can make an attack less likely. Deterrence still has a place in U.S. security policy.

Private sector preparedness. Maritime transportation system resilience and risk management means that private sector owners and operators of high-risk maritime transportation facilities have robust emergency preparedness and continuity of business plans and capabilities. The 9/11 Commission recommended that private sector preparedness be mandatory:

“We endorse the American National Standards Institute’s recommended standard for private preparedness. We were encouraged by [then] Secretary Tom Ridge’s praise of the standard, and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company’s compliance with the ANSI standard in assessing its insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money and national security.”³⁴

Wider implementation of emergency preparedness and continuity of business plans and capabilities by the private sector will help significantly reduce the consequences of a terrorist attack, mitigating both individual losses and the broader impact on the U.S. economy. As part of the MIRP effort, risk-based assessments of maritime transportation facilities should address their emergency preparedness and continuity of business as well as security programs.

To recap, the optimum strategy for protecting maritime transportation would take a risk-based approach to integrating security, consequence reduction, and emergency preparedness and continuity of business into comprehensive plans and programs for enhancing the resilience of the maritime transportation system. This approach also would strongly support the objectives and policies contained in the recently-published “Interim National Preparedness Goal,” which is a major step in implementing Homeland Security Presidential Directive 8 (HSPD-8), “National Preparedness.”³⁵ The United States cannot make every facility that is part of the maritime transportation system an impregnable fortress, but it can do much to enhance the resilience of the system and mitigate the consequences of an attack.

Enhance and Fund the Port Security Grant Program

As was described earlier, the Port Security Grant Program has serious problems and changes to the program proposed by the Bush Administration will only make matters worse. Five measures are needed to enable the Port Security

Grant Program to achieve the goals set under the MTSA:

- Maintain independent port security grant program;
- Allocate grants directly from DHS to recipients;
- Adopt a better risk-based approach to grant allocation;
- Broaden grant fund use and impact; and
- Increase funding levels commensurate with MTSA implementation requirements.

Maintain independent program. Because the Port Security Grant Program supports a specific statutory mandate imposed on a single industry, it should remain an independent program and not be merged with other grant programs. Merging port security grants within the proposed virtually guarantees that scarce resources will be spread too thin across various critical infrastructure sectors that should not be in competition.

All of the other critical infrastructures covered by TIP have significant security-related funding requirements, as do state and local law enforcement and first responders.³⁶ Comparing the \$600 million requested for the TIP Grant Program in fiscal year 2006 with the \$315 million appropriated for port, rail, mass transit, trucking industry and inter-city bus grant programs in fiscal year 2005 is misleading. It really is not an increase, as has been claimed by the Bush administration. State and local law enforcement and first responders are facing deep cuts, from \$5.71 billion in fiscal year 2005 to only \$3.57 billion in fiscal year 2006.³⁷ Those funds have to be replaced. If the MTSA is to have the desired impact – meaningful security enhancements and risk mitigation steps that keep our people, communities and economy safe, then it needs a dedicated source of funding to support implementation.

Allocate grants directly to recipients. Responding to intense pressure from state governments,³⁸ the Bush Administration has proposed that TIP funds be allocated to the states.³⁹ State governments would then decide which TIP grant applications would be funded, simply shifting the competition for grant funds from the federal to the state level, where the competition will be much more politicized.

There are a number of reasons to retain the current distribution method. The U.S. Coast Guard is responsible for MTSA implementation and also reviews, along with the Maritime Administration, Customs and Border Protection and others, all port security grant applications. It is in the best position to match available funding with port security priorities. No comparable national maritime perspective exists at the state level. States should be consulted as called for in the current port security grant guidance.⁴⁰ However, given the unique national

economic impact that ports have, and the on-going federal responsibility for implementation (and authority to sanction any port or facility not in compliance), it makes sense to maintain a centralized approach.

Adopt a better risk-based approach to grant allocation. The risk assessment approach to port security, concentrating on the threat and consequences of a terrorist attack, should also be used to set priorities for grant applications and fund allocation. Ports and facilities that are required to meet higher standards should receive the highest priority when it comes to grant funding. Nonetheless, while high-impact major ports may well qualify for the majority of available funds, the system must take into account individual high-risk facilities at smaller ports as well.

Broaden grant fund use and impact. Currently, the increased cost of personnel, operations, maintenance and training required for compliance with MTSA and Coast Guard regulations must be borne solely by port authorities and private port facility operators. Yet compliance with MTSA has significantly increased annual operating expenses, including maintenance of new high tech security systems, training and exercise expenses and associated personnel costs. Federal compensation for overtime costs incurred when DHS raises its alert status to the Level Orange is not sufficient.

The rules governing the Port Security Grant Program should be amended to permit a portion of those funds to be applied to annual operating expenses for security. A formula could easily be developed that permits port authorities and private facility operators to apply for grants to cover a portion of their annual operating expenses for security, based on the security enhancements they have made in order to comply with MTSA. In addition to calculating requirements for capital investments to enhance security, grant funding must also incorporate what port authorities need to maintain MTSA compliance and help defray at least some of those annual costs. The Port Security Grant Program also should be employed to encourage greater attention to risk management, emergency preparedness and continuity of business capabilities.

Increase funding for MTSA implementation and long-term sustainability. Meeting MTSA mandates and implementing Coast Guard Maritime Facility Security Regulations requires a significant financial commitment. It is not a financial obligation that ports can avoid because of potential MTSA and Coast Guard fines or sanctions. Yet MTSA-mandated security measures are far more extensive and demanding than those the maritime transportation industry would implement for the security of their own facilities based on a routine risk management approach.⁴¹ Clearly, the intent of MTSA is to

protect the nation from terrorist attacks – both attacks facilitated by smuggling weapons of mass destruction through seaports and attacks intended to cripple the American economy by forcing large-scale closure of seaports. In short, the maritime transportation industry has been mandated by federal law to protect the entire nation against terrorist attacks.

Although MTSA placed significant responsibility for homeland security on the shoulders of the port industry, the federal government has not provided funding commensurate with that responsibility. DHS should increase annual funding for the Port Security Grant Program to \$500 million per year to ensure proper MTSA implementation. If an effective risk-based strategy is adopted, where low-risk maritime transportation facilities have security requirements that are more appropriate to the threat – and affordable – the cost of MTSA compliance probably could fall below the current Coast Guard estimate of \$7.3 billion over ten years. Any long-term estimate must take into account the extent to which the program is broadened to cover additional requirements. The key point is to provide sufficient funding that matches the critical importance of maritime security to the people and economy of the United States.

Finally, to ensure MTSA implementation and sustainability over the long term, adequate funding is essential. Port security is too important to remain hostage to annual budget submissions and competing demands. The federal government should establish a port security trust fund into which 3-5% of the \$15.2 billion in customs revenues collected on goods moving through the nation's ports each year would be placed. Allocation of those funds would be via a process incorporating the best features of the current Port Security Grant Program, particularly the review of funding requests by subject matter experts, and applying the enhanced risk-based approach to setting priorities described earlier. Such an approach is consistent with dedicated funding arrangements for other transportation priorities, such as the security fee added to all airline tickets.

PORT SECURITY AND THE WAR ON TERROR

Progress in enhancing maritime transportation security has been impeded by missteps in the war on terror. The Bush Administration strategy for protecting the United States against the threat of terrorism places overwhelming emphasis on taking the offensive against terrorists overseas. President Bush made this point in a speech on port security in Charleston in February 2004:

“...the best way to defend the homeland is to stay on the offensive. The best way to protect America is to find the killers and bring them to justice before they ever harm another American – and that's exactly what this administration will continue to do.”⁴²

The President and Vice President have reiterated this strategy multiple times this year, at least in part to counter growing criticism of the failure of their Iraq policy.⁴³ Vice President Cheney's recent claim that the Iraqi insurgents were in their "last throes" is simply not credible.⁴⁴ Although taking the offensive against terrorists may appeal to the Republican conservative political base (though less every day to the American public⁴⁵), it is not, in and of itself, a viable strategy for protecting the United States against the threat of terrorism. The current stress that is evident within our military forces, and the strain that operations in Iraq and Afghanistan on the federal budget, suggest strongly that after Iraq, we will require a strategic pause and a change in approach. The question is whether we are doing what is necessary now to make our homeland more secure. The answer is no.

Actions speak louder than words and budget priorities speak loudest of all. The Bush administration is spending much less on homeland security than it is in Iraq, which has become an inspiration and training ground for a new generation of terrorists – much in the same way that Afghanistan was after the Soviet invasion.⁴⁶ Our current strategy of taking the offensive against terrorists and rogue regimes accurately (in the case of the Taliban in Afghanistan) or inaccurately (in the case of Iraq) perceived as supporting al Qaeda has increased the long-term terrorist threat to the United States. By starving homeland security initiatives of badly needed funds, it has exacerbated our vulnerability here at home.

The United States needs to find a better approach to integrating the various dimensions of our national power and reach a better balance between offense and defense. We cannot win the war on terror just through military operations overseas, but we can lose the war on terror through vulnerability and inattention at home. Enhancing homeland security not only contributes to protecting Americans from attack at home, it contributes to winning the war on terror by forcing potential attackers to devote much greater time and resources to planning and executing an attack – thus increasing our opportunities to detect and stop them.

CONCLUSION

Port security is a national imperative and requires a national approach. Since the benefits of maritime operations extend to 50 states, we should have a system where the costs of better security are shared across the country. That is what a genuine partnership really does. The federal government, states, municipalities and private owners and operators are now all players in our global system of commerce and all have responsibilities to help secure it. But only the federal government can set up appropriate mechanisms so that the burden is spread appropriately across the system and is thus sustainable over the long-term. The current approach fails to achieve that goal. A new approach is necessary.

Although MTSA was badly needed to correct the long-standing neglect of maritime transportation security, one year later it is clear that serious flaws that must be corrected if we are to achieve effective security and, more importantly, robust ability to minimize the consequences of a terrorist attack. Implementation of MTSA has been hampered by the Bush Administration's reluctance to devote adequate resources to the task. Because maritime transportation security is an unfunded mandate, we are less secure and more vulnerable than we should be as we approach the fourth anniversary of September 11. Now is the time to rectify these shortcomings, before rather than after another successful terrorist attack.

About the Author

Dr. Bouchard joined Zel Technologies, LLC (ZELTECH) as Executive Director of the Center for Homeland Security and Defense (CHSD) upon retiring as a United States Navy Captain in 2003 after twenty-seven years of active duty service. He was a Surface Warfare Officer, serving in destroyers and frigates and commanding the destroyer USS OLDENDORF (DD 972), and a specialist in strategic, long-range and operational planning, including a variety of assignments at The White House, NATO and the Pentagon. At the National Security Council, he was principal author of the National Security Strategy between 1997 and 1999, and was responsible for national security telecommunications and port security matters, including Presidential Decision Directive 40 on security of U.S. seaports. He served as White House representative to the U.S. Coast Guard's inter-agency Port Security Committee and in the Navy Operations Group, which is responsible for planning the Navy's role in the war of terror.

Dr. Bouchard gained wide recognition as an expert on port security while Commanding Officer of Naval Station Norfolk. He testified before the House Armed Service Committee, Special Oversight Panel on Terrorism in June 2001 on U.S. Navy port security and force protection efforts. He was co-developer (with the Coast Guard Captain of the Port) of the Joint Harbor Operations Center (JHOC), which integrated the Coast Guard and Navy with other federal, state and local law enforcement agencies for effective port security in Hampton Roads. The JHOC they developed has become the model for providing security in all U.S. ports.

Dr. Bouchard graduated with distinction from the U.S. Naval Academy, where he majored in International Security Affairs. He earned a Master of Arts degree in National Security Affairs from the U.S. Naval Postgraduate School, and a Doctor of Philosophy in Political Science from Stanford University, concentration in international relations and strategic studies. He is the author of Command in Crisis, published by Columbia University Press.

Acknowledgements

This paper was commissioned by the Center for American Progress as part of its Critical Infrastructure Security Series. Editorial direction and production assistance were provided by P.J. Crowley, senior fellow and director of national defense and homeland security; Matt Brown, production manager; and Ben Armbruster, research associate.

Endnotes

¹ The International Maritime Organization passed Assembly Resolution A.584(14) in 1986 on “Measures to Prevent Unlawful Acts Against Passengers and Crews On Board Ships.”

² The American Association of Port Authorities, the American Society for Industrial Security, the U.S. Department of Transportation and other organizations published guidance on terminal, cargo and port security in the 1980s and 1990s.

³ Report of the Interagency Commission on Crime and Security in U.S. Seaports (Washington, DC: U.S. Government Printing Office, Fall 2000).

⁴ Congressional Record – Senate, July 20, 2001, pp. S8015-S8022; John Frittelli, Maritime Security: Overview of Issues (Washington, DC: Congressional Research Service, December 5, 2003), pp. 1-2; Maritime Transportation Security Act of 2002, Public Law 107-295, November 25, 2002 (Washington, DC: U.S. Government Printing Office, 2002), cited hereafter as “MTSA 2002.”

⁵ U.S. House of Representatives, Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, Hearing on Implementation of the Maritime Transportation Security Act, June 9, 2002, pp. 1-2, available at <http://www.house.gov/transportation/cgmt/06-09-04/06-09-04memo.html>; Frittelli, pp. 2-3; Statement of Admiral Thomas H. Collins, Commandant, U.S. Coast Guard, Robert C. Bonner, Commissioner, U.S. Customs and Border Protection, and Rear Admiral David M. Stone, Acting Administrator, Transportation Security Administration, on Maritime Security Status before the Committee on Commerce, Science and Transportation, U.S. Senate, March 24, 2004, p. 2; Department of Homeland Security, “Secure Seas, Open Ports: Keeping Our Waters Safe, Secure and Open for Business,” June 21, 2004, p. 1; Margaret T. Wrightson, Testimony before the Committee on Commerce, Science and Transportation, U.S. Senate, “Maritime Security: Enhancements made, but Implementation and Sustainability Remain Key Challenges,” May 17, 2005 (Washington, DC: Government Accounting Office, May 17, 2005), p. 4-5; Department of Homeland Security, U.S. Coast Guard, “Statement of Rear Admiral Larry Hereth on Port Security,” before the Committee on Commerce, Science and Transportation, U.S. Senate, May 17, 2005, p. 2; Robert C. Bonner, Commissioner, U.S. Customs and Border Protection, Statement, Hearing before the Permanent Subcommittee on Investigations, Senate Committee on Homeland Security and Government Affairs, May 26, 2005, p. 2. Statistics on maritime transportation vary across sources due to differences in exactly what is being measured and the manner in which they are presented. For example, in December 2002 the Coast Guard estimated that 4,365 facilities were covered by MTSA; in June 2004 the number was 3,200 or 3,500, depending on who was speaking on what date; and in May 2005 the number was 3,100. The exact value of the figures is not the issue. What is important is that they are all very large. All sources agree on that.

⁶ Fiscal Policy Institute, “Economic Impact of the September 11 World Trade Center Attack,” (New York: Fiscal Policy Institute, September 28, 2001); Robert Looney, “Economic Costs to the United States Stemming From the 9/11 Attacks,” Strategic Insight (Monterey, CA: Center for Contemporary Conflict, August 5, 2002), available at <http://www.ccc.nps.navy.mil/si/aug02/homeland.pdf>; General Accounting Office, “Review of Studies of the Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center” (Washington, DC: General Accounting Office, May 2002).

⁷ Council on Foreign Relations, “America Still Unprepared – America Still in Danger,” (New York: Council on Foreign Relations, 2002), p. 23; Mark Gerencser, Jim Weinberg and Don Vincent, “Port Security War Game: Implications for U.S. Supply Chains,” (McLean, VA: Booz Allen Hamilton, 2002), pp. 3, 5; Michael E. O’Hanlon, et. al., Protecting the American Homeland: A Preliminary Analysis (Washington, DC: Brookings Institution, May 2002) pp. 6-7, available at <http://www.brook.edu/fp/projects/homeland/chapter1.pdf>; Stephen S. Cohen, “Economic Impact of a west Coast Dock Shutdown” (Berkeley, CA: University of California at Berkeley, January 2002), pp. 11-12, available at <http://brie.berkeley.edu/~briewww/publications/>

ships%202002%20final.pdf; Patrick L. Anderson, “Lost Earnings due to the West Coast Port Shutdown – Preliminary Estimate” (Lansing, MI: Anderson Economic Group, LLC, October 7, 2002), pp. 1-2; Wally Baker, “The OnTrac Trade Impact Study: Implications for Communities, Manufacturers and Retailers” (Los Angeles, CA: Los Angeles Economic Development Corporation, February 15, 2005), pp. 8-9, available at http://www.laedc.org/data/pdf/laedc_021505_ontractradeimpactstudy.pdf; Amy Zeigert, et. al., “Port Security: Improving Emergency Response Capabilities at the Ports of Los Angeles and Long Beach,” California Policy Options 2005 (Los Angeles, CA: University of California Los Angeles, School of Public Affairs, 2005), p. 181; Wrightson, p. 5. For views that the economic cost of the Los Angeles/Long Beach dock worker lockout may have been overestimated, see Sam Zuckerman, “Shutdown not so bad after all,” San Francisco Chronicle, October 18, 2002, available at <http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2002/10/18/BU197898.DTL>; Evelyn Iritani and Marla Dickerson, “Tallying Port Dispute’s Cost,” Los Angeles Times, November 25, 2002, p. 1; Peter V. Hall, “‘We’d Have to Sink the Ships’: Impact Studies and the 2002 West Coast Port Lockout,” Economic Development Quarterly (vol. 18, 2004) pp. 354-367. The lower estimates are based on the fact that the lockout only closed a single port for a finite period of time and was the result of a labor dispute rather than a terrorist attack, which meant normal operations could resume as soon as the labor dispute was resolved. The destruction of port infrastructure and extensive loss of life resulting from a terrorist attack would cause recovery to take much longer and thus cause much greater economic loss.

⁸ My estimate of the economic consequences of shutting all U.S. ports rises rapidly over the first 45 days due to two factors. First, inventories held by manufacturers, wholesalers and retailers are rapidly exhausted during that period. Second, if all U.S. ports had to remain closed for a month or more, energy shortages quickly become acute. Sea borne oil imports provide 62% of U.S. consumption. Domestic production increase could only compensate for a small fraction of lost imports. Stocks on hand average about 700 million barrels, which would last about 45 days at normal consumption rates. The Strategic Petroleum Reserve (about 700 million barrels) can only provide 4.3 million barrels per day, about 20% of U.S. daily consumption. After 90 days, daily deliveries from the Strategic Petroleum Reserve rapidly decline to 1.3 million barrels per day (6.5% of US daily consumption) until the reserve is exhausted. Liquid petroleum products account for only 3% of electrical generation. The primary impact would be on transportation, which would suffer catastrophic losses due to price gouging by the oil industry and shortages. Natural gas consumption in 2003 was 21.9Tcf (trillion cubic feet). Natural gas storage capacity in the United States is about 1.1 Bcf (billion cubic feet). Natural gas imports in 2003 were 3.8Tcf, most from Canada via pipeline. Sea borne liquefied natural gas (LNG) imports were 507 Bcf, about 2.3% of consumption. Increased domestic production and imports from Canada probably could compensate for loss of sea borne LNG imports. The impact of halting sea borne LNG shipments would be regional in the areas serviced by the three U.S. LNG terminals (Lake Charles, Louisiana; Elba Island, Georgia; and Cove Point, Maryland). However, increased demand for natural gas to compensate for the oil shortage (58% of natural gas consumption is by electrical generation and industry) probably would cause natural gas prices to skyrocket, further exacerbating the decline of U.S. economy. Oil and natural gas data are from various reports and tables available from the Energy Information Administration, Department of Energy, at <http://www.eia.doe.gov/>.

⁹ Maritime Transportation Security Act of 2002, Public Law 107-295, November 25, 2002 (Washington, DC: U.S. Government Printing Office, 2002), Section 101(13). Further insight into the purpose and goals of the act can be found in Senator Ernest F. Hollings, Statement on introduced bill S. 1214, Congressional Record – Senate, July 20, 2001, pp. S8015-S8017.

¹⁰ Code of Federal Regulations, Volume 33, Navigation and Navigable Waters, Chapter I, Coast Guard, Department of Homeland Security, Subchapter H, Maritime Security. Cited hereafter as “Coast Guard Maritime Security Regulations.”

¹¹ U.S. Coast Guard, “Notice of meetings; request for comments,” December 30, 2002, Federal Register, vol. 67, pp. 79742-79781.

¹² U.S. Coast Guard, Navigation and Vessel Inspection Circular No. 03-03, “Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities,” December 15, 2003; U.S. Coast Guard, Navigation and Vessel Inspection Circular No. 03-03, Ch. 1, “Change 1 to NVIC 03-03, Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities,” May 27, 2004.

¹³ Secretary of Homeland Security Tom Ridge, “Remarks by Secretary Tom Ridge at the Port of Los Angeles,” June 21, 2004, available at <http://www.dhs.gov/dhspublic/display?theme=44&content=3728&print=true>.

15. U.S. Department of Homeland Security, Office of Inspector General, “Review of the Port Security Grant Program,” OIG-05-10, January 2005.

¹⁴ MTSA, Section 102, amendment to Title 46, United States Code, Section 70107, paragraph (a).

¹⁵ Ibid, paragraph (b).

¹⁶ U.S. Coast Guard, “Notice of meetings; request for comments,” Appendix C, “Cost Analysis Report for Vessel, Facility and Port Security,” December 30, 2002, Federal Register, vol. 67, pp. 79782, 79795, 79805; Department of Homeland Security, “Statement of Admiral Thomas H. Collins, Commandant, U.S. Coast Guard, Robert C. Bonner, Commissioner, Customs and Border Protection, and Admiral David M. Stone, Acting Administrator, Transportation Security Administration, on Maritime Security Status,” Committee on Commerce, Science and Transportation, U.S. Senate, March 24, 2004, p. 12.

¹⁷ American Association of Port Authorities, “New Port Security Regulations will Require Billions in Investment,” October 23, 2003, available at <http://www.aapa-ports.org/pressroom/oct2303.htm>; American Association of Port Authorities, “AAPA Concerned FY ’05 Budget Lacks Funds for Port Facility Security,” February 2, 2004, available at <http://www.aapa-ports.org/pressroom/feb0204.htm>; American Association of Port Authorities, “AAPA Welcomes Availability of Seaport Security Funds,” May 13, 2005, available at <http://www.aapa-ports.org/pressroom/may1305.htm>; Jean Godwin, “Testimony of Jean Godwin, Executive Vice President and General Counsel, American Association of Port Authorities,” before the Committee on Commerce, Science and Transportation, U.S. Senate, May 17, 2005, pp. 2, 4.

¹⁸ On January 14, 2004 President George W. Bush announced that the United States would send a manned mission back to the moon no later than 2020, possibly as early as 2015, to be followed by landing an astronaut on Mars. Although he did not give a date for the Mars landing, specialists in space exploration estimate that at funding levels requested by NASA, it could be achieved by 2030. President George W. Bush, “A Renewed Spirit of Discovery: The President’s Vision for U.S. Space Exploration,” January 14, 2004, available at http://www.whitehouse.gov/space/renewed_spirit.html; The White House, “Fact sheet: A Renewed Spirit of Discovery,” January 14, 2004, available at <http://www.whitehouse.gov/news/releases/2004/01/20040114-1.html>; National Aeronautics and Space Administration, The Vision for Space Exploration, February 2004, available at http://www.nasa.gov/pdf/55583main_vision_space_exploration2.pdf; Professor Colin Pillinger, “Toward a manned mission to mars,” CNN, May 25, 2005, available at http://www.cnn.com/2005/TECH/space/05/12/visionary.pillinger/index.html?section=cnn_latest.

¹⁹ American Association of Port Authorities, “Comparison of Federal Port Security Grants to Funding Proposals, Rounds 1-5,” in “Legislative Priorities: Seaport Security” (Alexandria, VA: American Association of Port Authorities, April 2005), p. 2.

²⁰ West Coast ports are already experiencing significant congestion. “LA, LB Port ‘congestion’ Surcharges Levied,” The CalTrade Report, November 16, 2004, available at <http://www.cal-tradereport.com/eWebObjects/print-version.cgi?dynamic=http://www.caltradereport.com/eWebPages/page-two-1100322931.html>; George Raine, “Ports just keep getting busier,” *San Francisco Chronicle*, March 6, 2005, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/03/06/BUGP0BKUM91.DTL&hw=port+congestion&sn=002&sc=937>

; Ronald D. White, "Growing Problems Give Ports a Bad Reputation," *Los Angeles Times*, May 4, 2005. p. C1; Peter Robison, "Imports choke Los Angeles port," *The Standard* (China's Business Newspaper), Friday, May 13, 2005. At least one shipping company has advised shippers to allow an extra seven days for deliveries through the Port of Los Angeles due to port congestion. See DHL, "Los Angeles Port Congestion," *DHL News*, September 14, 2004, available at <http://www.us.danzas.com/frameset.cgi?winLocation=http://www.us.danzas.com/worldwide/northamerica/resource/450.html>. Visit the web sites for the Port of Los Angeles (<http://www.portoflosangeles.org/>) and Port of Long Beach (<http://www.polb.com/>) for overviews of their ambitious expansion plans.

²¹ U.S. Department of Homeland Security, Office of Inspector General, "Review of the Port Security Grant Program," OIG-05-10, January 2005; U.S. Department of Homeland Security, "Statement of Richard L. Skinner, Acting Inspector General, U.S. Department of Homeland Security," before the Committee on Commerce, Science and Transportation, U.S. Senate, May 17, 2005.

²² U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, "FY 2005 Port Security Grant Program: Program Guidelines and Application Kit," May 2005, pp. 3-4, 7-8. Cited hereafter as "FY 2005 Port Security Grant Guidelines."

²³ *Ibid*, p. 6

²⁴ *Ibid*, pp. 10-11.

²⁵ U.S. Coast Guard, "Notice of meetings; request for comments," Appendix C, "Cost Analysis Report for Vessel, Facility and Port Security," December 30, 2002, Federal Register, vol. 67, p. 79795.

²⁶ U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, "FY 2005 Port Security Grant Program: Program Guidelines and Application Kit," May 2005, pp. 5-8.

²⁷ U.S. Department of Homeland Security, "Budget in Brief: Fiscal Year 2006," February 7, 2005, pp. 6, 82.

²⁸ Keever, p. 22.

²⁹ MTSA 2002, Section 70102.

³⁰ This led many facility operators to ask why on earth they were required to perform the extensive security assessment when they had no option but to comply with the mandated universal security requirements regardless of the outcome of the assessment.

³¹ Homeland Security Presidential Directive 13 (HSPD-13), "Maritime Security Policy," December 21, 2004, pp. 3, 7-8.

³² Although HSPD-13 mentions developing "contingency plans to continue the flow of commerce in the event of an incident necessitating total or partial closure of U.S. borders to maritime commerce" (p. 9), those plans are not part of the MIRP and will not achieve the integration of security and continuity of operations advocated in this paper.

³³ Henry H. Willis and David S. Ortiz, "Evaluating the Security of the Global Containerized Supply Chain" (Santa Monica, CA: The RAND Corporation, 2004), pp. 25-26.

³⁴ National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition (New York: W.W. Norton & Co., 2004), p. 398. The American National Standards Institute standard is National Fire Protection Association, "Standard on Disaster/Emergency Management and Business Continuity Programs," NFPA 1600, 2004 Edition (Quincy, MA: National Fire Protection Association, 2004).

³⁵ Department of Homeland Security, "Interim National Preparedness Goal," March 31, 2005, available at http://www.ojp.usdoj.gov/odp/docs/InterimNationalPreparednessGoal_03-31-05_1.pdf; Homeland Security Presidential Directive 8 (HSPD-8), "National Preparedness," December 17, 2003, available at <http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>.

³⁶ A brief overview of just one other critical infrastructure covered by TIP – chemical plants – will illustrate the magnitude of the increased competition. Concern for the security of chemical plants is well founded. According to the Environmental Protection Agency, 123 chemical facilities in the United States each threaten a million or more nearby residents. More than 700 plants could put at least 100,000 people at risk and more than 3,000 facilities have at least 10,000 people nearby. Press reports indicate that copies of U.S. chemical industry trade publications were found in an al Qaeda hideout in December 2001. DHS has not published an estimate as to how much it would cost to secure all U.S. chemical plants that could threaten neighboring populations, but the American Chemistry Council, whose members operate only about 7% of those plants, claims to have spent \$800 million on security upgrades in 2003 alone. Although the total cost for security upgrades is not a linear extrapolation from that figure, clearly the total cost is in the billions of dollars – \$5 billion would be a very conservative estimate. That estimate is the same order of magnitude as estimates for the port industry to comply with MTSA. Clearly, funding the TIP Grant program at only \$600 million is woefully inadequate to meet the needs of the port and chemical industries alone, not to mention the other sectors of the transportation industry, nuclear power plants and the rest of the energy industry, and other critical infrastructures covered by TIP. Department of Homeland Security, “Fact Sheet: Protecting America’s Critical Infrastructure – Chemical Security,” April 26, 2005, available at <http://www.dhs.gov/dhspublic/display?theme=43&content=4480&print=true>. Data on chemical industry is from the American Chemistry Council, available at <http://www.accnewsmedia.com/site/page.asp?TRACKID=&VID=1&CID=361&DID=1313&PSID=ACC>. Also see Carl Prine, “Chemical Sites Still Vulnerable,” Pittsburgh Tribune-Review, November 16, 2003, available at http://pittsburghlive.com/x/search/s_165532.html.

³⁷ The assistance provided to state and local governments in fiscal year 2005 includes the Urban Area Security Initiative, Homeland Security Grant Program, Law Enforcement Terrorism Prevention Program, Emergency Management Performance Grants, Citizen Corps Grants and Metropolitan Medical Response System Grants, Training, Exercises and Technical Assistance Program, Fire Fighter Assistance Program, Technology Transfer Program, and the Department of Justice Community Oriented Policing Services (COPS) and Byrne Justice Assistance programs. In fiscal year 2005, the total of all those grants is \$5.71 billion; in fiscal year 2006, only \$3.57 billion has been requested for those programs – including the TIP Grant Program. That represents an overall 37% reduction in homeland security grants. See U.S. Department of Homeland Security, “Budget in Brief: Fiscal Year 2006,” February 7, 2005.

³⁸ National Governors Association, Executive Committee Paper 5, “Homeland Security Comprehensive Policy,” 2003, available at http://www.nga.org/nga/legislativeUpdate/1,1169,C_POLICY_POSITION^D_5102,00.html; Governors Ruth Ann Minner and Mitt Romney, Co-Lead Governors for Homeland Security, National Governors Association, letter to Senator Susan M. Collins, Chair, Senate Governmental Affairs Committee, October 19, 2004, available at http://www.nga.org/nga/legislativeUpdate/1,1169,C_LETTER^D_7448,00.html. The National Conference of State Legislatures also is on record that all homeland security grant funds should be distributed via the states. National Conference of State Legislatures, “Homeland Security Funding: An Underfunded National Expectation,” policy position for 2004-2005 Goals for State Federal Action, available at <http://www.ncsl.org/statefed/fedbud.htm#HomelandSecurity>.

³⁹ U.S. Department of Homeland Security, “Budget in Brief: Fiscal Year 2006,” February 7, 2005, pp. 6, 82.

⁴⁰ FY 2005 Port Security Grant Guidelines, pp. 7-8. The provision for state government participation is consistent with Executive Order 12372, “Intergovernmental Review of Federal Programs,” which was issued to include state governments in the review of proposed Federal financial assistance under various grant programs.

⁴¹ For example, the Virginia Port Authority’s security program costs \$6 million per year, which includes almost \$1 million in overtime for the Port Authority Police – a cost difficult to avoid given the manpower-intensive security procedures mandated by the Coast Guard regulations.

Prior to MTSA, VPA spent well under \$4 million per year and enjoyed a decade without an incident of cargo theft on any of its terminals. This clearly illustrates the difference in cost between a security program designed to meet a port's crime prevention requirements, and a homeland security program designed to protect the security of the American people. Jeff Keever, Deputy Executive Director, Virginia Port Authority, Statement before the Subcommittee on Crime, Terrorism and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, March 15, 2005, P. 24.

⁴² President George W. Bush, "Remarks by the President on Seaport and Cargo Security," Charleston, South Carolina, February 5, 2004, available at <http://www.whitehouse.gov/news/releases/2004/02/print/20040205.html>.

⁴³ President George W. Bush, "President Discusses War on Terror," remarks at the National Defense University, Washington, DC, March 8, 2005, available at <http://www.whitehouse.gov/news/releases/2005/03/print/20050308-3.html>; President George W. Bush, "President Discusses War on Terror at Naval Academy Commencement," remarks at Navy Marine Corps Memorial Stadium, Annapolis, MD, May 27, 2005, available at <http://www.whitehouse.gov/news/releases/2005/05/print/20050527.html>; Vice President Richard Cheney, "Vice President's Remarks at United States Air Force Academy Commencement," United States Air Force Academy, Colorado Springs, CO, June 1, 2005, available at <http://www.whitehouse.gov/news/releases/2005/06/print/20050601.html>.

⁴⁴ Vice President Richard Cheney, "Interview with Dick Cheney, Lynne Cheney," CNN Larry King Live, May 30, 2005, available at <http://transcripts.cnn.com/TRANSCRIPTS/0505/30/lkl.01.html>; James Glanz and Thom Shanker, "Iraq Study Sees Rebels' Attacks as Widespread," New York Times, September 29, 2004, p. 1; Tom Lasseter and Jonathan S. Landay, "Analysis: Iraqi Insurgency Grows larger, More Effective," Knight Ridder Newspapers, January 23, 2005; Bradley Graham, "Army Plans To Keep Iraq Troop Level Through '06," The Washington Post, January 25, 2005, p. A1; Ann Scott Tyson, "Two Years later, Iraq War Drains Military," The Washington Post, March 19, 2005, p. A10; Bradley Graham, "U.S. Officers In Iraq Put Priority on Extremists," The Washington Post, May 9, 2005, p. A1.

⁴⁵ Susan B. Glasser, "Review May Shift terror Tactics," The Washington Post, May 29, 2005, p. A1; Jim VandeHei and Peter Baker, "Bush's Optimism on Iraq Debated," The Washington Post, June 5, 2005, p. A1; Dana Milbank and Claudia Deane, "Poll finds Dimmer View of Iraq War," The Washington Post, June 8, 2005, p. A1.

⁴⁶ Dana Priest and Josh White, "War Helps Recruit Terrorists, Hill Told," The Washington Post, February 17, 2005, p. A1; Susan B. Glasser, "'Martyrs' in Iraq Mostly Saudis," The Washington Post, May 15, 2005, p. A1. For a more optimistic view, see Dana Priest and Spencer Hsu, "U.S. Sees Drop in Terrorist Threats," The Washington Post, May 1, 2005, p. A1. Note that none of the officials quoted in this article was willing to declare victory in the war on terror and a number of them warned that we could be expe

Center for American Progress



ABOUT THE CENTER FOR AMERICAN PROGRESS

The Center for American Progress is a nonpartisan research and educational institute dedicated to promoting a strong, just and free America that ensures opportunity for all. We believe that Americans are bound together by a common commitment to these values and we aspire to ensure that our national policies reflect these values. We work to find progressive and pragmatic solutions to significant domestic and international problems and develop policy proposals that foster a government that is “of the people, by the people, and for the people.”

Center for American Progress
1333 H Street, N.W., 10th Floor
Washington, D.C. 20005
(202) 682-1611
www.americanprogress.org