

7. HOMELAND SECURITY

Three years after the 9/11 attacks, critical infrastructure in the United States remains as vulnerable as it was three years ago. Chief among those vulnerable systems are ports and shipping containers, rails (both freight and passenger), and chemical plants. In the major metropolitan areas, emergency services personnel (police, fire, medical) continue to lack minimum essential equipment, training, staff, plans, and technologies. Moreover, the current block-grant federal assistance program does not identify minimum essential capabilities or guarantee that basic requirements will ever be met. Finally, there has been no effort to identify the gaps between state and local capabilities and the systems required to address major catastrophic events, such as nuclear or biological attacks.

The 9/11 terrorist attacks highlighted the fact that our borders and oceans are not effective barriers for terrorists who plot to attack within U.S. borders. While American soldiers continue to sacrifice in conflicts overseas, few sacrifices have been undertaken to reduce vulnerabilities at home. This section highlights some of our greatest weaknesses and offers a pragmatic policy response for each.

SECURING PORTS AND CONTAINERS

The United States has numerous vulnerabilities, but our 361 seaports, which connect us to the world and handle 90 percent of everything moving in and out of our country, remain especially inviting to terrorists. And, unfortunately, our ports are as critical to homeland security as they are vulnerable to attack. Unsecured ports, and the 16,000 shipping containers that move through them every day, provide terrorists with a means of transporting weapons, people, and potentially deadlier contraband into the United States. In addition, vulnerable ports provide

terrorists with a means of bringing the entire international trade system to its knees. In 2002, approximately 7 million containers arrived at U.S. seaports, accounting for more than 75 percent of the U.S. non-North America trade by value and 95 percent by weight. A 2002 simulation of a terrorist attack involving cargo containers demonstrated that if every seaport were shut down temporarily due to such an attack, the estimated loss in revenue to the U.S. economy would be \$58 billion.

Because the threat has obvious national security implications, it deserves high-level attention at all levels of government. But the issue continues to receive an insufficient response, despite the importance of global transportation to our national interests and the monumental task of securing and monitoring the 7 million containers shipped through U.S. ports each year. Today, only 2 percent of those containers are inspected.

The key to efficient port security is identifying high-risk containers rapidly and dealing with them effectively, without impeding the flow of container traffic through the port facility. Failing to identify and deal with a high-risk container could be disastrous, but frequently disrupting container traffic could have its own deleterious effects on the economy. Given the volume of container traffic and the difficulty of conducting thorough inspections, meeting these requirements is a tall order.

PRACTICAL LIMITS

Large container ships can receive and discharge more than 6 million pounds of freight in a single hour. Today, the two largest container ports in the world, Hong Kong and Singapore, together handle more than 1 million forty-foot ocean containers each month. Moreover, on the average day, more than 15 million containers are moving by vessel, truck, or train, or awaiting delivery. As mega-container ships capable of carrying upward of 3,000 forty-foot containers were put into operation in the 1990s, the need to choreograph the movement of the boxes in and out of a marine terminal became more time-sensitive. Today's rapidly moving operations make the system very susceptible to disruptions. If many containers get held up in the off-loading process, the trains and trucks carrying boxes to the port will be trapped outside the terminal gate. If they are carrying perishable freight, it will spoil and become useless. The

most serious economic blow, however, would be dealt to the manufacturing and retail sectors. Because 90 percent of the world's general cargo moves inside these boxes, when they slow down or stop, so do assembly lines and retailers such as Wal-Mart and Home Depot.

For this reason, inspecting every container that comes through our ports would be impractical. In the aftermath of 9/11, however, legislation was introduced in Congress that would require every container entering the United States to be unloaded and examined. It takes five agents three hours to completely inspect a fully loaded forty-foot cargo container. On an average day, 18,000 containers are off-loaded in the ports of Los Angeles and Long Beach, California, alone. If every box were unloaded and inspected, meeting the proposed 100-percent inspection mandate would translate into 270,000 man-hours per day—which would require more than three times the customs inspection manpower that currently exists nationwide.

Moreover, even if we could inspect every container that came through our ports, container security would still not be ensured. On average, overseas containers will pass through seventeen intermediate points before they arrive at their final U.S. destination, and often their contents come from several locations before they are even loaded into the box. Nearly 40 percent of all containers shipped to the United States are the maritime transportation equivalent of the back of a United Parcel Service (UPS) van. Intermediaries, known as consolidators, gather goods or packages from a variety of customers or even other intermediaries and load them all into the container. Just like express carriers in the United States, they only know what their customers tell them about what they are shipping. Explosives, even weapons of mass destruction, could easily be loaded into a container at its point of origin or anywhere along the way to the marine terminal. Port terminal operators have no way of confirming whether what is advertised as the contents of a box is what is actually in it.

SECURING CONTAINERS IN THREE STEPS

Securing cargo containers requires three steps. First, only authorized goods should be allowed to be loaded into a container. Second, once a container is moving within the global transportation system, the shipment should be

impervious to an unauthorized breach. Third, each port should be capable of rapidly inspecting any cargo containers that arouse suspicion.

The U.S. government has taken numerous steps since the 9/11 attacks to improve container and port security. The International Ship and Port Facility Security Code (ISPS) recently came into force, marking the dawn of a new age for maritime security. Now, 22,539 vessels and the 7,974 port facilities that serve as their on-ramps and off-ramps should be abiding by new security measures adopted by the International Maritime Organization. Congress gave the code the force of law when it adopted the Maritime Transportation Security Act of 2002. But the new mandate has not come with the resources required to meet it. Since 9/11, Washington has provided only \$516 million toward the \$5.6 billion the Coast Guard estimates U.S. ports need to make them minimally secure. In the fiscal 2005 budget, the White House asked for just \$50 million more. Given the severe constraints on the state and local budgets within the jurisdictions where America's commercial seaports are located, it is difficult to see how these ports will be able to afford the new security requirements.

Another program, the Container Security Initiative (CSI) places Customs and Border Protection (CBP) staff at the largest foreign seaports to identify and inspect high-risk containers before they are shipped to the United States. Over twenty-four ports, including all the largest seaports in the world, have signed agreements to participate in the CSI program. However, CBP is staffing the CSI program by sending teams of just four to eight inspectors on temporary duty assignments of three to four months because the White House has not authorized the overseas billets for longer assignments. Inspectors are receiving no formal language or other training to prepare them for these overseas postings. Given that the teams are so small—only eight inspectors in Hong Kong, which is the world largest port—they are able to inspect only the tiniest of percentages of containers. Moreover, CSI uses ships' manifest data, which the Government Accountability Office (GAO) called "one of the least reliable or useful for targeting purposes," to evaluate risk.

The CBP also uses the National Targeting Center to alert customs inspectors in a port to hold selected boxes until they can be examined. Using the Automated Targeting System (ATS), the National Targeting Center evaluates information found on the cargo container manifest and the customs declaration form and correlates it with intelligence. CBP officials then use this information to identify high-risk containers for

additional scrutiny. Although the ATS was originally designed to identify illegal narcotics shipments, it has been modified to identify many more types of illegal contraband.

CBP also employs the Supply Chain Stratified Examination, which randomly selects containers for inspection. CBP officials have the capacity to conduct a nonintrusive inspection with equipment such as the Vehicle and Cargo Inspection System (VACIS), which takes a gamma-ray image of the target container. This system cuts down on inspection man-hours by distinguishing between trusted and untrusted boxes.

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected. By the end of 2003, 4,600 importers, ocean carriers, and freight forwarders had submitted applications to join C-TPAT.

The speed with which the CSI and C-TPAT initiatives have been embraced is not difficult to explain. Both importers and foreign port authorities fear that U.S. inspectors will subject shipments from non-participating companies and ports to greater scrutiny, with the associated delays. But these fears are largely unfounded, because the Bureau of Customs and Border Protection lacks the manpower and resources to adequately staff the CSI, to review applications of companies that wish to participate in C-TPAT, and to move away from error-prone cargo manifests that remain the cornerstone of the targeting system.

A NEW PLAN

The shipping networks we rely on today are integrated into much larger global systems. Thus, to fully secure our ports and the integrity of our global transportation system, we would need to harden all the key nodes in the transportation network. America's borders represent only a territorial line where our sovereign jurisdiction begins, but the threat to container security starts much farther back.

Virtually all containers coming into the United States pass through a few foreign seaports. In fact, approximately 70 percent of the 8 million containers that arrived in U.S. ports in 2002 originated from or moved through four overseas terminal operators. These operators, Hutchinson

Port Holdings, P&O Ports, PSA Corporation, and Maersk-Sealand, are the second-to-last line of defense, and they should ensure that only secure boxes are loaded on ships that cross the Atlantic and Pacific oceans. Their job would involve two steps. First, they should confirm that a low-risk container is in fact low-risk; if it is deemed high-risk, it should be handled in a way that minimizes danger and disruption.

Guaranteeing that a container has not been tampered with will become much easier if we can ensure that the container was loaded in a secure facility at its point of origin. Secure facilities should have loading docks with safeguards that prevent anyone from gaining unauthorized entry. When the container is being loaded, digital photographs with time signatures could record the interior of the container at four stages: when it is empty, half full, full, and after the security seal is activated. These photographs would be stored on a data chip with the container or be transmitted electronically to the authorities in the loading port. The container could have additional sensors: light, temperature, and pressure sensors that could detect an unauthorized intrusion, and internal sensors that could detect gamma or neutron emissions associated with a nuclear or dirty bomb, prohibited chemical and biological agents, or the carbon dioxide generated by smuggled persons.

Using global positioning system (GPS) technology, the container's route could be tracked over sea and land. When in transit over land, if a truck driver is going through areas known for smuggling or terrorist activities, a form of invisible fence technology could be outfitted inside the truck. A microcomputer could detect whether the truck strayed from its route, send an alert message to the relevant authorities, and later automatically idle the engine before the truck arrived at the port terminal.

When a container arrives at a terminal, an inspection unit would create a CAT scan-style image of its contents, detect any radiation, and gather information from the container's sensors, and do all of this non-intrusively. These data would be forwarded electronically to all the national customs authorities along the route. With multiple sets of eyes monitoring containers en route, the chance of a high-risk container penetrating the system would be dramatically reduced.

To ensure that each container is traveling on its advertised route, authorities will need to track the shipment over sea and land. Most Americans would be surprised to learn that although civilian air-traffic controllers can track aircraft, there is no equivalent system for monitoring movement of ocean-going ships, let alone the containers aboard those

ships. Creating this capability is technologically feasible, but it has never been mandated. Although large ships must carry a device that allows the Coast Guard to detect them when they are near U.S. shores, the device can only track ships within twenty to thirty miles of the coast.

There are several ways the U.S. government could establish a container tracking system. The first option is to use a GPS-based system that would send a signal to a transmitter on each container and receive a signal from that transmitter regarding its location, using a different technology. The second option is to place Radio Frequency Identification (RFID) tags on each container, which would be able to receive and send transmissions, but only when the container is moving through “choke points” at marine and terrestrial terminals. The third option is to use space-based radars to establish “globally persistent” surveillance systems that can provide a real-time picture of anything that can be seen from space. This technology is not currently available for the container security task. But were it to be developed for such a task, it would provide the greatest resolution and tracking capability of all three options.

Using new technologies and procedures to check and double-check containers will serve several purposes. First, they will create a deterrent against terrorists shipping a nuclear weapon in a container. With increased scrutiny of containers via sensors and more vigorous monitoring, we could push the probability of detection from its current 10-percent range into the 90-percent range. Given the difficulty of obtaining a nuclear weapon, a terrorist organization would be less likely to take such a risk. Outfitting containers so they could be tracked would provide the means to act on intelligence about high-risk containers without disrupting the rest of the transportation system.

The cost for all this would be reasonable. Assuming that the average container is used for ten years, the initial cost of installing sensor technology into the box would add about \$5 to the price of each shipment. The latest radiation-detection portals and container-scanning equipment units cost about \$1 million each. Large ports would need several to ensure that the screening process would not slow the flow of container traffic. Ports should also have spares on hand to allow for routine maintenance. New command centers with upgraded technology and good analysts would be the backbone of a secure network to share and analyze the scanned images across multiple jurisdictions.

Some of the costs of security can be passed on to the private sector by providing appropriate incentives. One initiative could be establishing “green lanes” in seaports. The green lane would be similar to the E-Z Pass toll collection system on the highway. A green lane in a seaport would be authorized only for secure containers whose location could be tracked. The benefits to the shipper would come in several ways. First, the users of the green lane would be provided with assurances from the U.S. authorities that these boxes would receive preferential treatment if their shipment were targeted for inspection, thereby minimizing delays for that shipper. Second, should the United States temporarily have to shut down ports following a terrorist attack, once the ports were reopened those shippers with green lane privileges would be authorized to move first.

SECURING OUR TRAINS

The Madrid commuter train attacks that killed 191 people on March 11, 2004, exposed the extreme vulnerability of public transportation systems. Since the attacks, the U.S. Transportation Security Administration (TSA) has been testing more rigorous security measures on some commuter trains, including bomb-screening machines, random bag checks, and patrols with bomb-sniffing dogs. These efforts are sporadic, however, and the U.S. government has not allocated funding necessary for sustained and effective security measures.

Journalists from ABC News ran an experiment in September 2004 to assess security on commuter trains in the United States. The journalists were able to leave several backpacks conspicuously unattended, à la Madrid, in three different commuter trains in Washington, D.C., Virginia, and New York, without raising suspicion, for two hours in one case. Although security is slowly improving, terrorists could very easily attack many vulnerable points in our system.

The 32 million Americans who use public transportation every day deserve more thorough protection from terrorist attacks. An American Public Transportation Association (APTA) survey found that the United States will have to spend \$6 billion to secure the nation’s transit systems. Since 9/11, however, only \$155 million has been appropriated by

Congress for this effort—which is about 1 percent of the funding appropriated for aviation security, even though every day sixteen times as many people travel by public transportation as by air.

Although Congress has introduced legislation designed to increase transportation security, including block-grant programs, a number of congressional leaders have delayed passage of the bills. The next administration has the opportunity to play a critical role in this process by ensuring the passage of a block-grant program dedicated to enhancing transit system security, focusing in particular on subways, commuter trains, and Amtrak railways.

SECURING CHEMICAL FACILITIES

According to the Environmental Protection Agency, there are 7,728 U.S. chemical plants in which an accident—or act of sabotage—could endanger 1,000 or more nearby residents. Of those, 123 facilities could threaten more than 1 million people. More recent assessments by the Department of Homeland Security (DHS) conclude that the number of plants threatening 1,000 or more people has been lowered to 4,391, while the number potentially affecting more than 1 million has dropped to two. A GAO report released in March 2003 noted that even though U.S. chemical facilities were “attractive targets for terrorists,” the ability of any facility to respond to an attack was “unknown.” The GAO found that the chemical industry was not required by law to assess vulnerabilities or take action to secure its facilities and that “the federal government has not comprehensively assessed the chemical industry’s vulnerabilities to terrorist attacks.” The problem is that the efforts are ultimately dependent on the willingness of plant owners and managers to work with Homeland Security officials and spend money and time on the efforts. DHS currently has no ability to force security measures on the industry.

The Justice Department calls the threat “real and credible.” Yet the chemical industry is not required by law to assess vulnerabilities or secure its facilities. The *Richmond Times-Dispatch* reported that “the Environmental Protection Agency recently tried to impose stricter security standards on chemical manufacturers, but it backed down after the industry balked.”¹

SUPPORTING EMERGENCY RESPONDERS

Local and state emergency responders are a vital component of America's front line in homeland security. First responders play a central role in managing the immediate response to a terrorist attack, and their efforts in the initial minutes following an attack will determine how many lives are saved and how quickly order is restored. The nation's emergency responders, like military field medics, have been asked to place themselves in harm's way to defend and rescue the wounded on the battlefield of the twenty-first century. Unfortunately, America's emergency responders are underfunded and, as a result, unprepared for this duty. If the next administration does not take immediate steps to improve emergency responder capabilities, then the next attack on the U.S. homeland could be even more disastrous than the attacks on 9/11.

An independent task force, sponsored by the Council on Foreign Relations, issued a publication, "Emergency Responders: Drastically Underfunded, Dangerously Unprepared," which offers (1) a glimpse of America's critical deficits in emergency preparedness, and (2) recommendations for making up these deficits.

Before highlighting the deficiencies in our emergency responder system, it is important to note that since 9/11, the United States has made significant improvements in emergency preparedness. In March 2002, the Department of Homeland Security was established, and this effort was coupled with increased funding for emergency preparedness at the federal, state, and local levels and increased training for emergency response personnel. These initiatives are important and useful, but they are a far cry from what America requires to respond to the catastrophic emergencies, such as those involving chemical, biological, radiological, or nuclear agents, that now loom on the horizon.

To improve our emergency preparedness, we first need to strengthen the foundations of our emergency response system. Before we establish a higher bar for the emergency response system, we should first meet the current bar. For example, two-thirds of fire departments nationwide do not meet the consensus fire-service standard for minimum safe staffing levels. On average, fire departments have only 50 percent of the radios and one-third of the breathing apparatuses they need to equip all of the firefighters on one shift. Public health systems nationwide are underfunded and cannot meet the standards that they are increasingly required to meet.

An urgent task is to define, and then assess, the country's minimum essential capabilities for emergency responders. There is currently no systematic national standard of essential capabilities and therefore no way to assess how much progress we are making toward preparedness on the federal, state, or local level. More important, there is currently no way of determining which jurisdictions are suffering from critical gaps in preparedness and what steps those jurisdictions should be taking to make up the gaps. Once we have assessed our emergency preparedness, we can set systematic requirements for emergency responder systems nationwide, codified in national capability standards. The capability standards should include guidelines for burden sharing among federal, state, and local jurisdictions. Although the federal government should not be responsible for normal spending on emergency readiness and public health at the state and local levels, federal funds should be used to help state and local governments meet the essential standards for preparedness, uniquely designed to prepare jurisdictions for catastrophic terrorist attacks.

Improving emergency preparedness also requires that we provide the funds necessary to equip and train emergency responders and implement programs critical to responding to mass destruction events. According to the Council on Foreign Relations' task force, the United States will fall approximately \$98.4 billion short of meeting emergency responder needs over the next five years if current funding levels are maintained. These shortfalls in funding translate into dangerous deficits, given the scope and character of the terrorism threat. For example, only 10 percent of fire departments nationwide have personnel and equipment to handle a building collapse; police departments throughout the United States do not have protective gear required to secure a site after an attack with weapons of mass destruction (WMD); public health laboratories in most states do not have the basic equipment to adequately respond to chemical or biological attacks; and most cities do not have the equipment needed to determine which hazardous agents emergency responders are facing following an attack.

Other programs the task force factors into "emergency responder needs" include implementing a nationwide emergency-911 system with wireless capability; enhancing urban search and rescue capabilities of major cities in cases where buildings or other large structures collapse; implementing interoperable communications systems for emergency responders; enhancing public health preparedness by strengthening

laboratories, disease tracking, and training for public health personnel for dealing with biological, chemical, and radiological events; providing protective gear and WMD remediation equipment to firefighters; enhancing emergency agricultural and veterinary capabilities to respond to a national food supply attack; and enhancing the surge capacity of the nation's hospitals.

Specialized training for emergency personnel and sustaining equipment capabilities over time are also required to be fully prepared. New equipment will only have a marginal effect on preparedness if personnel are not trained to use it effectively or if it is not maintained well. In fact, many state and local governments have been unwilling to accept federal funding for programs that will generate long-term costs without the promise of federal funding to cover those costs. Because state and local governments will continue to leave themselves unprepared for fear of getting stuck with the bill, the U.S. government needs to guarantee sustained multiyear funding for critical preparedness programs.

Federal funding of state and local homeland security should be requirements-based. For each major metropolitan area, there should be a clear target of minimum essential capabilities to respond to a catastrophic terrorist attack and a multiyear funding plan to achieve those minimum essential capabilities.

Refocusing our funding priorities is another way to keep our emergency preparedness programs cost effective. For example, the U.S. government currently disburses emergency preparedness funds according to a minimum level due to each state, plus additional funds based on a state's population. This formula has led to some very uneven funding. Wyoming receives \$10 per capita while New York state receives \$1.40 per capita, from the Department of Homeland Security. Although all Americans are equally deserving of protection, some Americans live in high-risk areas and some in lower-risk areas, and preparedness funding should reflect this reality.

Improving emergency preparedness also requires that the U.S. government swiftly deliver assistance and funding to state and local governments. According to the Council on Foreign Relations task force, many metropolitan areas and states have actually received and spent a small portion of their congressionally appropriated emergency responder funds. State and local governments have complained that the increased amounts of paperwork, coupled with shifting federal requirements, have made accessing and efficiently spending preparedness funds

difficult. According to the National Emergency Managers Association, “appropriation cycles have been erratic, causing extreme burdens on state and local governments to continue preparedness activities when there is no federal funding, and then forcing them to thoughtfully and strategically apply several years of federal funds and millions of dollars at one time.”²

The U.S. government should also apply itself to disseminating best practices throughout the emergency responder communities. There is currently no formal mechanism through which emergency responders can share best practices and lessons learned, though the emergency responder community has expressed a great deal of interest in the idea. Centralizing and cataloging these data would surely improve the near-term quality of our response efforts and provide a long-term foundation upon which to base decisions about priorities, planning, training, and equipment.

If terrorists employ biological, chemical, or radiological agents in a catastrophic attack, the emergency response and rescue operations would be orders of magnitude more difficult and dangerous than those following 9/11. Improving our emergency preparedness by swiftly addressing funding and planning shortfalls may dramatically decrease civilian and emergency responder casualties should such an event transpire. September 11 demonstrated the great sacrifice our emergency responders have made, and continue to make, for America. To ensure that their continued sacrifice is not made in vain, we should provide them with the equipment and training they require to effectively and safely fulfill their duty.

