July 9, 2003

The Honorable Tom Ridge
Secretary
Department of Homeland Security
Washington, DC 20528

Dear Secretary Ridge:

I am writing to express my deep concern over the Administration's failure to address the serious gaps that exist in transportation security outside the field of passenger aviation. While the Transportation Security Administration (TSA) has made progress in and devoted resources to improving air passenger and baggage screening, this same level of commitment has not been evident in other modes of transportation such as rail, public transit, air cargo or maritime. Despite substantial documentation of the security deficiencies in these other areas, and widespread acknowledgment that security must be enhanced, little has been done by the Administration to remedy these vulnerabilities. Moreover, even within the area of passenger aviation, significant security challenges remain. It is time for the Administration to move beyond talk and take action to shore up the security of our transportation systems against attack.

Reports by independent experts and by the General Accounting Office (GAO) have identified substantial shortcomings in land and maritime transportation security that warrant immediate attention. For example, an independent task force report released in 2002 by the Council on Foreign Relations, "America - Still Unprepared, Still in Danger," warns that "only the tiniest percentage of containers, ships, trucks and trains that enter the United States each day are subject to examination - and a weapon of mass destruction could well be hidden among this cargo. Should the maritime or surface elements of America's global transportation system be used as a weapon-delivery device, the response right now would almost certainly be to shut the system down at an enormous cost to the economies of the United States and its trade partners." Recent testimony by GAO before the National Commission on Terrorist Attacks Upon the United States concluded that, while some progress has been made in passenger aviation transportation security, "major vulnerabilities remain, particularly in air cargo, general aviation, mass transit, and port security."[1] In the area of port security, for instance, the Coast Guard has identified billions of dollars worth of necessary improvements – and Congress has mandated enhancements – yet the Administration is not seeking significant funds to help make the changes.

---

[1] *Transportation Security: Post-September 11th Initiatives and Long-Term Challenges;* GAO-03-616T, April 1, 2003, at 20.

Stephen Flynn, a homeland security specialist at the Council on Foreign Relations, criticized the amount of funding dedicated to port security in a June 21, 2003 article in the *Boston Globe*: "A government that is wringing its hands over 1 or 2 million-dollar grants is still a nation that hasn't come to grips with the fact that the threat has changed. I was more forgiving in the first 18 months, but when you pass an act and you make sure there is no money to execute it, that goes beyond being slow to not taking this seriously."

By law, TSA is responsible for security in all modes of transportation.[2] In its first 1 ½ years of existence, TSA has focused almost exclusively on passenger aviation security concerns. Admiral James Loy, TSA Administrator, anticipated questions on TSA's broader mission in his testimony on May 13 before the Senate Appropriations Subcommittee on Homeland Security and stated that he was "close to the first draft of a national transportation system security plan." However, GAO noted in a report released on May 23 that "while the Transportation Security Administration has begun work on an overall intermodal transportation system security plan, it has not yet developed specific plans to address the security of individual surface transportation modes [such as rail or transit] and does not have time frames established for completing such an effort."[3]

We cannot afford to delay this action any longer. Threats to our security, our safety and our economy abound as a result of the vulnerabilities that currently exist in our transportation system. A stark example of the risks we face occurred in July 2001 when a 60-car train carrying flammable and toxic chemicals, acids and paper products derailed inside Baltimore's Howard Street Tunnel, which is on one of the major East Coast rail routes; the ensuing fire raged inside the tunnel for five days, traffic to the city was disrupted for several weeks, businesses in the area were forced to close during the emergency, and Baltimore incurred $4.5 million in overtime and materials costs. While the incident was not related to terrorism, it served notice of the vulnerabilities regarding hazardous materials in rail transport – vulnerabilities that terrorists might seek to exploit. According to GAO, more than 83 million tons of hazardous materials were shipped by rail in 2001.[4]

GAO has documented similar vulnerabilities in other transportation modes. In December 2002, GAO reported that numerous vulnerabilities have been identified in the air cargo system, including vulnerabilities in the security procedures of some air carriers and freight forwarders, and the potential for tampering with cargo during land transport to airports or at cargo-handling

---

[2] 49 USC §114(d).

[3] *Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed,* GAO-03-435, at 3.

[4] *Id* at 4.

facilities.[5] Also in December, GAO warned that mass transit systems, including subways and buses, are both "inherently vulnerable to terrorist attacks and difficult to secure."[6] And numerous experts, including GAO, the Council on Foreign Relations 2002 task force report, and the Brookings Institution have all highlighted the urgent need to shore up security at U.S. seaports, which are significant potential targets for terrorists by virtue of their vital role in global trade, proximity to metropolitan areas, and facilities intertwined with major petrochemical storage facilities. A 2002 Brookings Institution report observed that a weapon of mass destruction shipped by container or mail could cause damage or disruption costing the economy as much as $1 trillion.[7]

The Administration's apparent lack of commitment to taking concrete steps toward improved transportation security outside of passenger aviation is illustrated by its funding requests for TSA. The President's FY 2004 budget sought a $500 million decrease in funding for TSA from FY 2003 requested levels, on the grounds that certain one-time aviation security costs had been addressed. This is problematic on two fronts: first, many of these so-called one-time costs are ongoing; second, the budget indicates no commitment to broaden TSA's mission to other transportation modes. The FY 2004 TSA budget request seeks $4.3 billion for passenger aviation security, but only $86 million for maritime and land security. Moreover, this latter amount is largely dedicated to the transportation worker credentialing initiative and does not include funds for improving security in ports, mass transit or other high priority transportation security needs.

I am therefore requesting a full accounting of TSA's efforts to improve security in transportation. Please provide responses to the following questions by July 28:

Security Planning

1) A) What is the national transportation security plan, as described by Adm. Loy, designed to do and when will it be released?
   B) When will TSA release specific plans for protecting the security of individual surface transportation modes, such as mass transit and rail?

2) In June, 2002 the Transportation Research Board of the National Academies

---

[5] *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344, at 11.

[6] *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*, GAO-03-263.

[7] *Protecting the Homeland: A Preliminary Analysis*, Michael E. O'Hanlon et al., at 7.

issued *Special Report 270: Deterrence, Protection and Preparation: The New Transportation Security Imperative*. This report examined how security should be systematically integrated into our transportation system in the wake of the September 11 attacks and what role TSA can and should play in that process. A key recommendation of the report suggested that TSA establish a strategic research and planning office, distinct from its operational and enforcement responsibilities, that could (among other things) "devise and evaluate alternative security system concepts for the different modes of transportation" in collaboration with the public and private sector owners, operators and users, and encourage the integration of security goals and enhancements in transportation planning and design. Do you believe that such an office should be created by TSA? Please explain why or why not.

Transportation Security Funding

3) I am very concerned about the funding situation at TSA. On May 13, the TSA Administrator, Adm. Loy, stated in response to a question from Senator Murray before a Senate Appropriations subcommittee that he could not assure her that the $58 million appropriated for Operation Safe Commerce, a pilot program to improve security of shipping containers coming into the U.S., would be spent for that purpose. He indicated that the funds might be diverted to address a shortfall in the FY 2003 TSA budget. Adm. Loy informed the Senate Appropriations Subcommittee that TSA planned to cover cost overruns in aviation security by transferring not only funds dedicated for Operation Safe Commerce but also $105 million earmarked for port security grants. Although you recently committed to releasing the Operation Safe Commerce and port security grant money, TSA was actually seeking to reprogram funds to cover a funding shortfall that TSA estimates to be $913 million for FY 2003.

   A) When did TSA determine that it faced a funding shortfall for FY 2003? What expenses have contributed to this shortfall and when were those funds obligated?

   B) The Administration sought no additional funding for TSA in the FY 2003 war supplemental and requested a $500 million decrease in TSA's budget for FY 2004. Was TSA's FY 2003 funding shortfall considered when DHS submitted its homeland security funding requests for the emergency war supplemental and the FY 2004 budget? If so, how were these requests adjusted to meet TSA's expected funding needs?

   C) Please state what appropriated funds TSA is seeking to reprogram to cover this shortfall, including the purposes for which Congress appropriated those funds and what amounts TSA proposes to divert to the shortfall.

Coordination with the Private Sector

4) Many transportation assets - such as pipelines, rail and ships - are owned and controlled by the private sector. In a February 12, 2003 op-ed in the *Baltimore Sun*, Ivo Daalder, Michael O'Hanlon and Peter Orszag criticized the inadequate level of homeland security funding sought by the Administration for FY 2004. These senior fellows at Brookings, who co-authored the Brookings publication *Protecting the American Homeland*, stated: "The Bush Administration also still trusts the private sector to protect its own assets. But the business of business is business, not homeland security. Private markets will often not adequately protect against terrorist attack on their own ..." In fact, the failure of private airlines to perform adequate passenger and baggage screening led to the creation of TSA and the federalization of the screener workforce.

   A) To what extent does the Administration intend to rely on the private sector to take the lead on security in:
      - rail transportation
      - mass transit
      - highways
      - air cargo
      - pipelines
      - ports

   B) What steps does the Administration expect the private sector to take to improve transportation security in each of these modes and what will be the involvement of TSA in these efforts?

   C) How will the Department of Homeland Security (DHS) coordinate the efforts of private sector entities and federal, state and local agencies that share responsibility for security in areas such as seaports?

   D) What specific measures will DHS take to avoid the kinds of problems encountered when the private sector was responsible for passenger aviation security?

Port Security

5) The Maritime Transportation Security Act, P. L. 107-295, which was signed into law in November 2002, established requirements for improving the physical security of U.S. seaports. Despite Coast Guard estimates that it would cost $1 billion in the first year to implement physical security measures in ports and $4.4 billion over 10 years, the Administration has not supported funding to meet these needs. The Act requires the Secretary of Homeland Security (who assumed responsibility for the Coast Guard from the Secretary of Transportation) to prepare a funding proposal for correcting vulnerabilities in port security identified

by the Coast Guard and complying with port security plans in fiscal years 2003 through 2008. This report was due on May 25, 2003.

A) What is the status of this report and what amount of funding is the Administration requesting for port security for each of the fiscal years covered by this report?

B) What actions will DHS take to implement the requirements of this legislation in FY 2003 and FY 2004 and how will those actions be funded?

Air Cargo Security

6) According to GAO, billions of tons of cargo are transported each year on both passenger aircraft and all-cargo planes. In December 2002, GAO reported that numerous vulnerabilities have been identified in the air cargo system, including vulnerabilities in the security procedures of some air carriers and freight forwarders, and the potential for tampering with cargo during land transport to airports or at cargo-handling facilities.[8] GAO's report identified actions such as using explosives detection devices to screen cargo that could be used in the short term to improve cargo security and recommended that TSA develop a comprehensive long-term plan for air cargo security.

A) What actions will TSA take to ensure that cargo receives the same level of scrutiny that air passengers and baggage now receive?

B) What is TSA's timetable for putting these security measures in place? What short term measures is TSA taking? Has TSA developed a comprehensive long-term plan as recommended by GAO?

C) Are sufficient resources currently available to undertake these efforts and, if not, what will be required?

Mass Transit Security

7) According to a December 2002 GAO report, "terrorist events around the world have shown that mass transit systems, like other modes of transportation, are often targets of attack. For example, roughly one-third of terrorist attacks worldwide target transportation systems, and transit systems are the mode most commonly attacked."[9] One of the most notorious of these attacks was the 1995 attack on the Tokyo subway by a Japanese cult, Aum Shinrikyo. At the height of the Tokyo rush hour, members of the cult released sarin, a lethal chemical nerve gas, on 5

---

[8] *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344.

[9] GAO-03-263.

trains, killing 12 people and injuring 5500 more. According to a report on this attack by the Senate Governmental Affairs Permanent Subcommittee on Investigations, the attack caused widespread panic and chaos in the station and in Tokyo and could have easily killed tens of thousands if the Aum had not made some critical mistakes in carrying out its plan.[10] A similar attack in the U.S. could have devastating consequences not only through injury and loss of life but also on commerce, if the public's confidence in mass transit was severely shaken.

GAO's December 2002 report stated that "insufficient funding is the most significant challenge in making ... transit systems as safe and secure as possible" and estimated that the total cost of identified security improvements for eight transit agencies visited by GAO was roughly $711 million, with the price of securing all the nation's transit systems potentially reaching into the billions of dollars. Transit agencies across the country are strapped by tight budgets and have been unable to take many of the actions they feel are needed to improve security.[11] Although DHS recently announced it would distribute $65 million to the 20 largest transit agencies, this amount will not provide the help transit officials say they need.

A) What actions is DHS taking to secure:
   - subways
   - buses
   - commuter and light rail
   - ferries

B) How will DHS coordinate with state, local and regional authorities to improve mass transit security and what role do you expect state, local and regional authorities to play?

C) Has the Administration established standards or best practices for transit agencies to follow in improving security? If not, when will such guidance be available?

Rail Security

The July 2001 rail accident in Baltimore described above is only one example of the dangers present in our rail system today. Another event that demonstrated the potentially

[10] *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo* (October 31, 1995).

[11] "Transit Agencies Seek to Boost Subway Security - Tight Budgets Put Limits on Local Efforts to Guard Against Terrorist Attack," *Wall Street Journal,* May 28, 2003.

disastrous consequences of rail accidents occurred on April 11, 1996, when 19 cars from a Montana Rail Link freight train derailed near Alberton, MT. Six of the derailed cars contained hazardous materials, including chlorine (a poison gas), potassium hydroxide solution (a corrosive liquid) and sodium chlorate (an oxidizer). All of these substances were released in substantial quantity as a result of the accident, with serious consequences. According to a National Transportation Safety Board report on the event (RAB/98-07), about 1000 people from the surrounding area were evacuated, roughly 350 people were treated for chlorine inhalation (including 123 who sustained injury), 9 people were hospitalized and one died. The hazardous material cloud drifted across a nearby interstate highway, causing multiple traffic accidents and requiring the highway to be closed. The highway closure and evacuation were not lifted until chlorine was removed from the derailed but nonruptured tank cars, a process that was not completed until more than two weeks after the derailment. Monetary damages were estimated to be $3.9 million.

There is no doubt that the costs and impact of this event would have been far greater had it occurred in a more heavily populated area or one more central to transportation and commerce. The vast quantity of hazardous materials being transported by rail in the U.S., as documented by GAO (GAO-03-435), and its vulnerability to attack makes action to improve rail security crucial.

8) GAO's May 23 report on rail security noted a series of unresolved issues regarding the safety and security of transporting hazardous materials by rail. Most notably, the report cited the practice of "storage in transit," in which hazardous materials are temporarily stored in rail cars while awaiting delivery to their ultimate destination, and concluded that better measures are needed to safeguard these materials while they are being stored. In addition, the report raised questions about whether companies should be required to notify local communities about the type and quantities of materials being stored in transit and about other information regarding hazardous materials shipments passing through their communities. How does DHS plan to address rail security issues that potentially endanger local communities such as "storage in transit" of hazardous materials?

9) GAO also recommended that DHS work with the Department of Transportation to develop a risk-based plan that would help both Departments assess the adequacy of rail security measures already in place as well as identify gaps that need to be addressed. When will DHS complete a specific risk-based plan to address the security of rail transportation and what role will the Department of Transportation take in developing that plan?

10) In legislation reported out in the 107th Congress, the Senate Commerce Committee

identified a series of significant enhancements necessary to improve rail security, including infrastructure security improvements, such as the protection of tunnels, bridges and other rail facilities; rail equipment security, including improved communications, surveillance, and detection equipment; and system-wide security operations, such as hiring and training additional investigative and patrol personnel. The Committee also sought to authorize funds for a pilot program to provide random screening of passengers and baggage at certain major Amtrak stations and for a study of security and safety at stations served by Amtrak.

A) What action, if any, is DHS taking to address:
- rail infrastructure security improvements
- rail equipment security
- system-wide rail security operations
- random screening of rail passengers and baggage
- security and safety at stations served by Amtrak

B) Has DHS sought funding to address rail security, and if not, what is the Administration's timetable for making improvements in rail security?

Cybersecurity for Freight Transport

11) A June 2003 report by the National Research Council (NRC) of the National Academy of Sciences, "Cybersecurity of Freight Information Systems," describes the potential terrorist attacks that could be launched against our air, rail and trucking freight transportation cybersystems. Freight transport is a multi-trillion dollar industry which involves millions of trucks, rail cars and containers, and which employs millions of people to move billions of tons of freight every year. The report highlights the disruption and danger that could be caused by hacker terrorist attacks on these modes of transportation.

The NRC report states that "the freight transportation industry appears to offer unusual potential for both economic and physical damage from terrorist cyberattacks." It cites the 800,000 hazardous materials (hazmat) shipments that take place every single day in the U.S. as potential targets for terrorists. For example, terrorist hackers could locate and track such shipments and then attack them in locations where there could be a risk of high civilian casualties. Cyberattacks could possibly derail trains carrying hazmat. Terrorists also could manipulate information systems in order to bring weapons of mass destruction into the U.S. disguised as ordinary freight. While perhaps unlikely, these are legitimate concerns because the freight transport industry is becoming increasingly dependent on information technology (IT).

A) Is DHS addressing this issue of cybersecurity for freight transport IT systems? Is the Department of Transportation addressing this issue? What actions, if any, have been taken individually and together?

B) The NRC report states that priorities for protecting these IT systems must be set since implementation of protective measures will take time. Has DHS set those cybersecurity priorities? What cybersecurity measures are being implemented?

C) Is DHS doing any work to try to coordinate physical security measures, such as E-seals, with IT measures so that the physical security measures are protected from tampering done through cyber means?

D) Is DHS identifying and developing options to enhance cybersecurity for freight transport systems? How is DHS coordinating these efforts with the private sector?

E) The NRC report recommends a study to develop a strategy for possible steps to reduce the freight transport sector's vulnerability to terrorist cyber attacks in the least costly and disruptive way. Does DHS support such a study? Does DHS support the NRC's recommendation that industry be involved with federally funded research and development centers and academic research centers to do this study?

F) The NRC report seems to indicate that the analysis on the vulnerabilities, risks and consequences of potential terrorist cybersecurity attacks on the transportation systems handling freight shipments has not yet been done. Has DHS done any analysis of these issues and, if so, what are the results?

Aviation Security

12) TSA has announced plans to reduce its screener workforce this year by a total of 6000 positions. Three thousand of these positions were eliminated as of May 31 and the remaining cuts are scheduled to become effective by September 30. The screeners affected have completed the TSA screener training and have been deployed in airports across the country to screen passengers and baggage. While I understand that some positions will be cut by attrition and others will be terminated for cause, including undisclosed criminal histories, I expect that a substantial number of the remaining screeners are competent and qualified members of the workforce. Since TSA has made a substantial investment in hiring and training these individuals, I am concerned that TSA may be wasting government resources by eliminating these employees from the workforce without first determining whether their skills can be put to good use for other needed tasks. One option may be to utilize these workers to screen air cargo traveling on passenger aircraft, a current gap in aviation security about which GAO has raised

substantial concerns, as noted in question 6 above.

A) How many screeners scheduled to have their positions terminated would be qualified to remain on the TSA workforce if this reduction did not occur?
B) How much has it cost TSA to hire and train these employees?
C) How many such screeners currently work in airports that handle air cargo shipments on passenger aircraft? Is air cargo currently being screened for possible explosives in those airports?
D) TSA has announced that some screeners who might otherwise lose their jobs will be given an opportunity to apply for transfer to airports that need additional screeners for passenger and baggage duties. Apart from this plan, has TSA considered redeploying screeners whose positions are being terminated to other needed tasks, such as screening air cargo, in lieu of eliminating these positions?

13) A June 22 article in the *Washington Post*, "Airport Security Remains Porous," raised additional questions about the effect of the screener cutbacks on aviation security. The article also questioned whether TSA would be able to meet its extended deadline for scanning all baggage for explosives by machine by December 31, 2003.

A) The article stated that not all of the machines purchased by TSA to scan checked luggage for explosives are being used.
    1) How many explosives detection machines currently installed in airports are not being used to their full capacity?
    2) Have the reductions in the screener workforce led to reductions in the usage of these machines?
    3) What steps has TSA taken, and what additional steps if any will TSA take, to ensure that it has adequate numbers of trained screeners to staff these machines at full capacity?
    4) If there are other reasons these machines are not being used, or used to full capacity, please explain.
B) Section 425 of the Homeland Security Act directed TSA to report to Congress with a detailed plan on the deployment of explosives detection machines in airports that did not meet the original 2002 deadline, and to also submit interim reports on its progress in meeting this goal.
    1) Have these plans and reports been submitted on schedule? If not, why not?
    2) When will plans for installing explosives detection machines in all airports be completed?

3) When will all of the required machines be installed and operational?
4) Will there be any airports that have not completed installation of these machines by the end of 2003?
5) If so, when will all airports meet the requirement to have these machines installed and scanning baggage?

14) It was widely reported in late May 2003 that TSA had hired passenger screeners for airports that were later found to have disqualifying criminal backgrounds, including convictions for serious offenses such as felony gun possession and assault with a deadly weapon. As revealed in a June 3, 2003 House Homeland Security Appropriations Subcommittee hearing, in order to meet the November 2002 deadline for having a federalized screener workforce in place, TSA offered conditional employment to individuals who met the basic screener requirements. Based on a TSA briefing for Congressional staff, it is my understanding that these new screeners were trained and deployed in airports within two or three weeks after being interviewed for the position – but before TSA had completed background checks. Subsequently, the agency completed some of the pending background checks, found certain employees should not have been hired and fired them. Admiral Loy testified at the June 3 hearing that, as of May 31, 2003, TSA had terminated 1208 screeners for "suitability issues," including disqualifying criminal histories. That number will almost certainly rise: roughly half of the 53,500 screeners on the job still do not have completed background checks.

It is clear from this information that individuals who have been convicted of serious felonies received TSA training and were deployed in airports as passenger and baggage screeners. It would appear that, through their training and on-the-job experience, these individuals would have had access to highly sensitive aviation security information. For example, screeners are given information about the airport security program, which details all of the elements of security in an airport including how suspicious individuals are challenged. They are also instructed in screening protocols, such as the types of threat objects screeners look for. As a result of these individuals with criminal histories receiving access to this sensitive information, airport security procedures may have been compromised.

A) How does TSA assess the potential damage to its security procedures as a result of these events?
B) Has TSA sought to minimize any such damage? For instance, has TSA altered its security protocols so that the information these individuals have is no longer valid?

Container Security

15) Shipping containers present opportunities to smuggle and deliver many items that can pose significant threats to the U.S., including nuclear materials, explosives, biological or chemical weapons, and even terrorist operatives. An estimated six million containers of imported cargo were shipped to the United States in 2002. While several approaches have been announced by the Customs Service and its successor entities at DHS to address the security weaknesses in the international maritime shipping system, significant questions regarding the effectiveness of these methods remain.

A) Customs inspectors use an automated targeting system to determine which containers coming into a port present a high risk and should be inspected. This system, however, relies on a limited set of data found in the cargo manifest, which is provided by the shipper of the container based on information the shipper received from the shipping customer. This information is not independently verified, and reportedly some shipping customers may purposely provide vague information to deter theft of container contents. Moreover, if the container has traveled through multiple transshipment points, the shipper may not even know where the container originated. As a result, the targeting system is unable to reliably assess the risk posed by certain containers. Given the limitations of the information used in the automated targeting system, some experts have suggested that Customs Inspectors randomly select containers identified as low risk for inspection, to provide some uncertainty for those who are trying to evade inspection and perhaps reveal additional vulnerabilities that should be considered in this process. Are Customs Inspectors using a random selection system in addition to the automated targeting system for this purpose? If not, why not?

B) For many years, Customs has been developing a new computerized data system, the Automated Commercial Environment (ACE), that may allow more effective targeting and inspection of containers. When will ACE be fully up and running? Does DHS have sufficient resources to accomplish this? What barriers to completion remain?

C) Christopher Koch, President and CEO of the World Shipping Council, in an April 10, 2003 speech, called on Customs to "design its next generation import cargo processing system (the Automated Commercial Environment or ACE) to meet the government's security needs," saying that "the future requires the implementation of a different, more robust information system [than the current manifest system] that puts the obligation for providing transportation information on the carrier and the obligation for providing

cargo information on the shipper and consignee. The proper design and development of this new system should be a high priority for the U.S. government." Is the Department taking steps to go beyond the current manifest system and secure more detailed information about incoming shipping cargo? Please explain.

D) The Customs Service has initiated the Container Security Initiative (CSI) under which Customs inspectors are deployed to foreign ports to identify and inspect as much high-risk cargo as possible before it hits our harbors. The first phase of this program focused on 20 major ports in largely developed countries, such as Rotterdam and Singapore. Customs is now working to expand this program to significant ports in countries that have more limited resources and potentially significant problems including lack of technology. In order for this program to work effectively in these second phase ports, they will have to improve their available technology and provide a secure and reliable environment for inspections. How does the Department assess the challenge of expanding the CSI program to these additional ports? Please describe what measures are being taken to enable the program to operate effectively in these ports.

I appreciate your prompt attention to these concerns and look forward to your response. Please feel free to contact Susan Propper of my staff at (202) 224-6599 if you have any questions.

Sincerely,

Joseph I. Lieberman
Ranking Member