AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HOMELAND SECURITY: SECURING STRATEGIC PORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

JULY 23, 2002

Serial No. 107–216

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

87–388 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

ADAM H. PUTNAM, Florida
BENJAMIN A. GILMAN, New York
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia

DENNIS J. KUCINICH, Ohio
BERNARD SANDERS, Vermont
THOMAS H. ALLEN, Maine
TOM LANTOS, California
JOHN F. TIERNEY, Massachusetts
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
R. NICHOLAS PALARINO, *Senior Policy Advisor*
JASON CHUNG, *Clerk*
DAVID RAPALLO, *Minority Counsel*

CONTENTS

	Page
Hearing held on July 23, 2002	1
Statement of:	
Decker, Raymond, Director, Defense Capabilities and Management Team, U.S. General Accounting Office, accompanied by Joe Kirschbaum, Senior Analyst; and Kenneth Goulden, vice president, Maersk Sealand	54
Privratsky, Major General Kenneth L., Commander, Military Traffic Management Command, Department of Defense; Captain William G. Schubert, Maritime Administrator, Department of Transportation; and Rear Admiral Paul J. Pluta, Assistant Commandant for Marine Safety and Environmental Protection, U.S. Coast Guard, Department of Transportation	5
Letters, statements, etc., submitted for the record by:	
Decker, Raymond, Director, Defense Capabilities and Management Team, U.S. General Accounting Office, prepared statement of	57
Goulden, Kenneth, vice president, Maersk Sealand, prepared statement of	73
Pluta, Rear Admiral Paul J., Assistant Commandant for Marine Safety and Environmental Protection, U.S. Coast Guard, Department of Transportation, prepared statement of	34
Privratsky, Major General Kenneth L., Commander, Military Traffic Management Command, Department of Defense, prepared statement of	7
Schubert, Captain William G., Maritime Administrator, Department of Transportation, prepared statement of	24

HOMELAND SECURITY: SECURING STRATEGIC PORTS

TUESDAY, JULY 23, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Putnam, Gilman, Schrock, Tierney, Allen, Watson, and Lynch.

Staff present: Lawrence J. Halloran, staff director and counsel; R. Nicholas Palarino, senior policy advisor; Thomas Costa, professional staff member; Jason M. Chung, clerk; and David Rapallo, minority counsel.

Mr. SHAYS. A quorum being present, this hearing of the Subcommittee on National Security, Veterans Affairs and International Relations entitled, "Homeland Security: Protecting Strategic Ports," is called to order. I welcome our witnesses and I also welcome our guests.

This is the first of two hearings the subcommittee will convene on port security. Today we examine force protection measures and other precautions at the strategic seaports through which the bulk of U.S. military personnel and material pass in the event of a major mobilization. In 2 weeks, at Congressman Putnam's request, the subcommittee will hear testimony in Tampa, Florida, on security enhancements at critical commercial ports.

The deadly attacks on the U.S.S. Cole forced the Department of Defense to confront vulnerabilities of harbor operations abroad and at home. Even before that, the Inter-Agency Commission on Crime and Security in U.S. Seaports reported widespread, systemic weaknesses in procedures and policies to protect military property and personnel at the dock.

The Commission found security standards lacked consistency. Readiness is seldom tested in portwide exercises. Complex, unclear lines of authority between multiple Federal agencies, State regulators, local governments and private entities all but guarantee a fragmented, uncoordinated response to a portside attack.

More recently, the General Accounting Office surveyed a number of strategic seaports to assess security, management, and coordination. They found weaknesses in threat communication, risk mitigation, and resource allocation. Lack of end-to-end security planning

means some military equipment is completely outside DOD control during transit.

In this war, the front line is here at home. Last century's approaches to maritime security will not win the modern battle to secure strategic ports.

Our witnesses today will describe efforts to strengthen security planning and force protection at strategic seaports. We appreciate their time and the expertise they bring to our discussion of these important issues.

At this time I would recognize Mr. Schrock if he has any comment he would like to make.

Mr. SCHROCK. Thank you, Mr. Chairman, and thank you, gentlemen, for being here today.

I represent the Second Congressional District of Virginia, which includes Norfolk and Virginia Beach and will eventually include Virginia's eastern shore and a portion of Hampton. The District I represent boasts 384 military commands, eight major bases, including four four-star commands, and the giant Norfolk Naval Base.

Hampton Roads has the best natural deep-water harbor on the east coast of the United States. Fifty-foot deep unobstructed channels provide easy access and maneuvering room for the largest of today's container ships. The port is located just 18 miles from open sea on a year-round ice-free harbor.

The strategic location of the Port of Hampton Roads and its transportation infrastructure offer steamship lines and shippers access to two-thirds of the U.S. population. The Port of Hampton Roads transports more intermodal containers to more cities than any other port in the United States.

I have just described one of the most attractive terrorist targets in the United States. A ship sailing through Hampton Roads steams within a few hundred yards of the Norfolk Naval Base, home of the Atlantic Fleet, and Fort Monroe, home of the U.S. Army Training and Doctrine Command. Fort Eustis, home of the U.S. Transportation Command, is a short distance, a few miles up the James River.

The detonation of a ship-based weapon of mass destruction would have disastrous effects on our military and our economy. This is a nightmare we cannot allow. How are we going to prevent this scenario? Specifically, how are we going to keep these very lethal threats from endangering our ports of embarkation and military bases? That's what I'm hoping we can discuss today.

Every time I cross over the Hampton Roads Bridge Tunnel, as I did yesterday coming here, I think "what if," and the what-ifs scare me to death. Fortunately, I am starting to see signs of detectors on the bridge now, and that made me feel better than I have felt in a long time, but I know a lot more needs to be done, and I'm one who is willing to do anything I can to help solve this problem and prevent a disaster. That is my No. 1 issue in Congress right now—port security. We'll do anything to make sure our ports are secure.

Again, I thank you for being here. I thank you for what you're doing. I look forward to hearing your testimony.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

At this time the Chair would recognize the vice chairman of the committee, Mr. Putnam.

Mr. PUTNAM. Thank you, Mr. Chairman. I thank you for your leadership on this issue and your allowing the subcommittee to come down to Florida to focus in a second phase of this hearing on port security in our area.

As we focus today on the strategic seaports, these are those which offer the most attractive target to terrorists, as Mr. Schrock has pointed out, but they also offer what should be the most well-defended, well-guarded opportunities for terrorists to hit our seaports. I believe that there has been a pattern established where terrorists go after our more soft targets.

But it is disconcerting to note, as the GAO did, that even at these strategic seaports, which should be the best-defended, which should be the most well-guarded, there is no comprehensive process to mitigate vulnerabilities or prioritize resource distribution, no comprehensive mechanism for developing and communicating threat information, no mechanism in place to assess and communicate comprehensive threat information across agencies.

This is a recurring theme in our entire homeland defense and our entire national security strategy. Nobody is talking to anyone. There is no communication at any level. That, to me, is the most disturbing part of this entire GAO report and its entire discussion about homeland security.

While I, along with a lot of others, have pinned our hopes that the creation of a new department is going to improve communication and improve coordination, the bottom line is nobody is talking to each other now and we can only hope that they will begin to talk to each other in the future.

As we evaluate those threats of bio-terror release in one of the ports that would make incoming ships impossible to disembark in these ports and make the outgoing ships from the ports impossible to leave through quarantine or some other purpose; as we evaluate the threats of destroying a ship and clogging up the shipping panels; as we evaluate the patchwork of agencies—local, State, and Federal, Coast Guard and DOD—that share responsibility for these seaways, it becomes more and more clear that we have not adequately analyzed the threats that face our borders.

I look forward to the testimony today, and I thank the chairman for his leadership on this issue.

Mr. SHAYS. Thank you.

At this time the Chair recognizes Mr. Gilman, welcomes him. We welcome him and will hear his statement now if he would like to make one.

Mr. GILMAN. Thank you, Mr. Chairman.

Mr. SHAYS. You always come prepared, sir.

Mr. GILMAN. I thank you for holding this important and timely hearing. Due to events of September 11th and the attack on our U.S.S. Cole in Yemen, it has become increasingly clear that port security is an integral component within the broader context of our Nation's security and deserves much more attention than it has received in prior years as we work toward the consolidation of our homeland security responsibilities under a single Federal department.

It is imperative that we address this issue of port security. According to the GAO report, which is a focus of today's hearing, no single entity presently coordinates threat information among the myriad local, State, and Federal agencies with jurisdiction over our Nation's strategic seaports. Moreover, the GAO report asserts that the Department of Defense current system of protecting our Nation's military forces and equipment as they are deployed throughout our seaports is inadequately structured to today's security realities.

As the war on terrorism evolves, the likelihood that our Nation will deploy greater number of troops and equipment by way of these seaports is extremely high. Ensuring that our troops and equipment are not subject to sabotage, to theft, or attack on our own soil is essential. Accordingly, we welcome the testimony of today's distinguished panelists and hope that these participants can address the most critical issues regarding port security and the deployment of our Nation's military personnel and equipment through these vital seaports.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

Before I recognize our witnesses, I will take care of some housekeeping here and ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and that the record remain open for 3 days for that purpose. Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statements in the record. Without objection, so ordered.

At this time I will recognize our first panel. We have General Kenneth Privratsky, Commander, Military Traffic Management Command, Department of Defense; Captain William G. Schubert, Maritime Administrator, Department of Transportation; and we have Admiral Paul J. Pluta, Assistant Commandant for Marine Safety and Environmental Protection, U.S. Coast Guard, Department of Defense [sic], hopefully soon to be the Department of Homeland Security.

I would invite the witnesses to stand so I can swear you in, and then we will begin to hear your testimony.

[Witnesses sworn.]

Mr. SHAYS. We note for the record all three of our witnesses responded in the affirmative.

We will begin with you, General, and do welcome you here. Thank you for coming.

STATEMENTS OF MAJOR GENERAL KENNETH L. PRIVRATSKY, COMMANDER, MILITARY TRAFFIC MANAGEMENT COMMAND, DEPARTMENT OF DEFENSE; CAPTAIN WILLIAM G. SCHUBERT, MARITIME ADMINISTRATOR, DEPARTMENT OF TRANSPORTATION; AND REAR ADMIRAL PAUL J. PLUTA, ASSISTANT COMMANDANT FOR MARINE SAFETY AND ENVIRONMENTAL PROTECTION, U.S. COAST GUARD, DEPARTMENT OF TRANSPORTATION

General PRIVRATSKY. Mr. Chairman and members of the committee, thank you for the opportunity to speak today on the issue of

security as it relates to the movement of military cargo through strategic seaports. We have been blessed over the years with patriotic commercial port owners and operators, a robust strategic port infrastructure, excellent civil and military cooperation at all levels, and, until the events of September 11th, a relatively risk-free homeland. Like others appearing today, we in the Military Traffic Management Command have been reassessing requirements since that day.

I have submitted written comments for the record. In this opening statement, I would like to give you a sense of our ongoing efforts to keep deployments safe.

There are a significant number of players involved in the process of deploying units by sea. Considerable advanced planning and coordination is essential. One method used with success has been the National Port Readiness Committees. They create forums for everyone to understand clearly their roles and responsibilities and to surface potential issues or threats.

We in the Military Traffic Management Command also conduct extensive planning with deploying units, which includes identifying sensitive or hazardous cargos that may present special security concerns.

Because of GAO's assistance a year ago, we have made significant progress in safeguarding ammunition shipments to the Department of Defense's three ammunition ports. During deployments, events follow carefully scripted plans. They do not commingle with other commercial port activities. We have had lots of opportunity to practice. In the last 18 months, we have conducted 62 exercises or deployments, all without incident.

Following September 11th we added much emphasis. We asked for and received external assistance in assessing threats both at DOD-owned and commercial strategic ports, and we are implementing recommendations.

We in the Military Traffic Management Command are instituting a new port terminal risk analysis for use on each deployment operation. We also centralized command and control of operations at a single location at Ft. Eustis, Virginia, under the direction of a one-star general. That was something planned to be accomplished by June 2003. After September 11th, we accelerated our timeline. We now have a robust 24/7 operation managing surface transportation worldwide.

Prior to September 11th we had no significant intelligence capability within my command. Now we are adding that and have Reservists in our Operation Center in the interim developing intelligence. We routinely receive intelligence information from the Army military intelligence community and the U.S. Transportation Command. We have secure communications with some commercial carriers and associations to share information. As a result, we are much better prepared to see and communicate threats than we were last fall. All of us, however, remain on a journey at this point. We have made much progress, but there is certainly more that can and should be done. Toward that end, I look forward to seeing the results of GAO's examination on security measures. We will work hard to make our processes better.

I see positive developments in the legislation currently being worked by congressional conferees. Provisions directing Department of Transportation to assess the safety of all U.S. ports and to prepare anti-terrorism plans are critical. We agree with the need to have background checks and security identification issued by a central agency. We also are interested keenly in those measures that improve cargo identification and screening.

In closing, I would like to commend Congress for taking a national approach to port security. I appreciate the opportunity to appear before you today and I look forward to your questions.

Mr. PUTNAM [assuming Chair]. Thank you, General.

[The prepared statement of General Privratsky follows:]

RECORD VERSION

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE HOUSE COMMITTEE ON GOVERNMENT REFORM,
NATIONAL SECURITY, VETERANS' BENEFITS AND INTERNATIONAL
AFFAIRS SUBCOMMITTEE

STATEMENT OF

MAJOR GENERAL KENNETH L. PRIVRATSKY, USA
COMMANDER,
MILITARY TRAFFIC MANAGEMENT COMMAND

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM, SUBCOMMITTEE ON
NATIONAL SECURITY, VETERANS' AFFAIRS AND INTERNATIONAL RELATIONS
ON HOMELAND SECURITY; SECURING STRATEGIC PORTS

JULY 23 2002

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE HOUSE COMMITTEE ON GOVERNMENT REFORM,
NATIONAL SECURITY, VETERANS' BENEFITS AND INTERNATIONAL
AFFAIRS SUBCOMMITTEE

RECORD VERSION

STATEMENT

Mr. Chairman and Members of the Committee, on behalf of General Handy, I am appreciative of the opportunity to be with you today and provide testimony on the security coordination measures used by the Department of Defense at strategic seaports during mobilization of military personnel and cargo.

The Military Traffic Management Command (MTMC), headquartered in Alexandria, Virginia, is a major command of the Department of the Army and also a component of the United States Transportation Command (USTRANSCOM), headquartered at Scott Air Force Base, Illinois. The primary role of MTMC is to provide surface traffic management services for Defense agencies and military Services. As part of these overall services, we act as USTRANSCOM's seaport manager to organize and coordinate the movement of a wide range of cargo commodities used by the Department to carry out its global peacetime and wartime missions through both commercial and military seaports. The performance of that "Single Port Manager" mission involves extensive coordination and dependence on a number of interrelationships within the Department and among diverse federal and state agencies as well as commercial activities. All of these entities have vital roles to play.

Security is one of the most critical concerns of mobilization and deployment missions. Our ability to address threats to the national defense transportation network must be sufficient to meet the needs of agencies with Federal port responsibilities to deploy our nation's military forces swiftly and sustain them to meet national objectives. I will frequently use the term deployment in my testimony rather than mobilization. The reason for this is that mobilization is generally associated with a national call up, whereas deployments cover the range from peacetime exercises and contingencies to full mobilization.

Because of the excellent coordination among the many players involved in planning and executing deployments through our U.S. commercial ports, we have a long history of incident free deployments through what were normally considered low risk environments. Obviously, the terrorist attacks on September 11, 2001, raised the overall security concerns for Department personnel and cargo as well as for the public, and they caused us to review and in some cases revise past practices. Later in my statement, I will address some of those changes, but first I want to add some background and context on deployment operations.

DOD Role in Port Operations - Background Information

MTMC serves as the Single Port Manager for common-user ports and also, in most cases, as the Port Operator contracting with commercial stevedores to load or discharge vessels at those ports to deploy units or provide strategic supplies like ammunition, arms, and explosives. We maintain an active presence of military and civilian personnel in 24 commercial and military ports around the globe to support Defense Transportation System requirements. Nine of these ports are located in the Continental United States (CONUS). We often send Deployment Support Teams from these 24 ports to other ports as needed to facilitate operations. The teams range from a few personnel in some locations to dozens in others, all dependent on the mission to be performed. Our soldiers and civilian employees establish close communication and coordination on a day-to-day basis to enable the smooth and safe movement of Department forces. For contingency operations, active component elements provide the initial port management capability and then pass responsibility to our mobilized reserve units as they arrive. Port operators time their arrival so that they are sequenced with the arrival of deploying forces. About 55 percent of MTMC's force structure is in the reserves. We practice this seaport deployment process during unit movement exercises on a routine basis. In the past 18 months, we have conducted 62 exercises/deployments. Security planning and coordination is an integral part of that process.

In addition to coordinating security for unit deployments through U.S. ports, we manage the movement of arms, ammunition, and explosives through military ports. It is important to note that except in very small quantities during contingencies, arms, ammunition, and explosives are not moved through commercial ports. Almost all of this high-risk cargo is moved through military airfields or military port facilities in North Carolina, Washington and California. These port facilities are designed specifically for the movement of this cargo with significantly enhanced infrastructure and complete government control.

National Structure for Port Security Coordination - Background Information

To facilitate coordination within the Federal Agencies that support deploying forces in the event of a mobilization or national defense contingency, the National Port Readiness Network was created. An implementing memorandum between the Department of Defense and the Department of Transportation was executed to prescribe roles and responsibilities. This memorandum provided a forum for continuing coordination to promote more effective execution of the mission. The National Port Readiness Network process has enhanced coordination and cooperation among the following organizations at several echelons:

Maritime Administration	Joint Forces Command
HQ, Forces Command	U.S. Transportation Command
Military Sealift Command	Military Traffic Management Command
U.S. Army Corps of Engineers	U.S. Coast Guard
U.S. Maritime Defense Zone	

The National Port Readiness Network is made up of the National Port Readiness Network Steering Committee, the National Port Readiness Network Working Group, and all local Port Readiness Committees. The local committees are key to keeping all the players, including law enforcement, at a strategic port current on planning and operational issues through regular

meetings and port readiness exercises. MTMC is a participant at each level of the Network.

What and Where are Strategic Seaports - Background Information

Strategic seaports are U.S. ports designated to support major deployments under the National Port Readiness Network. These ports are chosen based on an evaluation of port capabilities compared to the military's deployment requirements. A team comprised of the Maritime Administration (MARAD) and MTMC selects the ports and establishes the number of vessel berths, staging areas, and other assets required. There are currently 17 designated strategic seaports. The 13 commercial ports are as follows: (1) New York/New Jersey Port Complex; (2) Hampton Roads Area Ports, VA; (3) Morehead City, NC; (4) Wilmington, NC; (5) Charleston, SC; (6) Savannah, GA; (7) Jacksonville, FL; (8) Beaumont, TX; (9) Corpus Christi TX; (10) San Diego, CA; (11) Long Beach, CA; (12) Oakland, CA; and (13) Tacoma, WA. The remaining four ports are Department of Defense facilities. They are: (1) the Military Ocean Terminal Sunny Point, NC; (2) the Military Ocean Terminal Concord, CA; (3) the Indian Island Naval Magazine, WA; and (4) the Naval Base Ventura County, Port Hueneme, CA. The first three Department facilities are specifically used for the movement of arms, ammunition, and explosives while the fourth is used for deploying units.

To facilitate deployment through these strategic ports in contingencies, Port Planning Orders have been issued to commercial port facility owners and/or operators. These orders, which are agreed to by port authorities, specifically identify the critical berths, warehouses, and staging areas required on short notice to support deployments.

Understanding the Deployment Process

There are two major pieces to any deployment - planning and execution. In the planning phase, units are identified and ports selected. That begins a series of coordination actions between

MTMC, which is the port planner and integrator; elements of the deploying units, which will be required to provide some level of port support activity and security; the Military Sealift Command (MSC), which will provide the vessels; the U.S. Coast Guard, which will provide water side security; and local port authorities and their assorted business and law enforcement partners, who will provide facilities, labor, and shore side security. At that point, preparations begin for addressing force protection or other security issues. These sessions often involve "terrain walks" to familiarize everyone with the process. MTMC uses a force protection checklist that covers everything from personnel, to lodging, to transportation, to communications, to operational site assessments. MTMC's force protection efforts focus on personnel working in the port area and equipment being prepared for deployment, not the broader category of deploying forces. Deploying forces normally move by air, separate from their unit equipment and do not transit the seaport.

In the execution stage, units are called forward according to a time-phased sequencing. They move from the fort to the port using a variety of methods - commercial truck, rail, or military road march. They pass through a controlled checkpoint at a gate or gates and are directed to a marshalling area. Meanwhile, vessel stow plans are being completed and ultimately equipment is moved to a staging area to be loaded aboard the vessel. At various times in this process, equipment is scanned for accountability purposes. From beginning to end, deployment is a very controlled process. Deployment activities are purposely segregated from other commercial port activities.

Procedures In Place During Mobilization To Protect Military Forces And Cargo Deploying Through Strategic Seaports

The Department has a number of internal and external procedures in place during mobilization to protect military forces and cargo deploying through strategic seaports. They involve a mix of Federal, State, local government agencies, and military and commercial entities, each with different but

complimentary responsibilities. The owners and/or operators of the ports and vessels have primary responsibility for the protection of their ports and vessels. Military unit commanders are responsible for equipment and resources under their command. Security of unit personnel and equipment in the U.S. is a Service responsibility under Title 10. Accordingly, deploying units provide security for their equipment and personnel until it reaches the designated theater. FBI and local law enforcement are responsible for protecting against terrorist acts and other civil disturbances, respectively. The U.S. Coast Guard as the Captain of the Port has overall enforcement responsibility. MTMC's MOU with the Coast Guard includes the Coast Guard's responsibility for waterside security and safety, as well as for HAZMAT concerns. The Coast Guard also has the responsibility of establishing safety zones by using all coordinating elements. Although the Coast Guard has responsibility for waterside security and safety, its ability to provide support in all cases may be limited due to current Coast Guard resource constraints and other significant Maritime Homeland Security mission requirements. MTMC coordinates with these organizations and shares information on force protection measures and requirements for the protection of personnel and equipment transiting through strategic commercial ports.

During a mobilization, the Port Readiness Committee establishes a command cell that is used to staff any issues that may arise. The Port Readiness MOU, dated 15 March 1999, clearly defines the duties of MARAD, JFCOM, FORSCOM, USTRANSCOM, MSC, MTMC, U.S. Army Corps of Engineers (USACE), USCG, and the U.S. Maritime Defense Zone. The port readiness committee consists of: DoD, the Department of Justice (FBI, INS, and DEA), Department of State, Department of Agriculture, U.S. Customs, Office of National Drug Control and Policy, MSC, MTMC, Federal Emergency Management Agency, the Environmental Protection Agency, MARAD, the intelligence community, and the maritime industry. Each agency of the Port Readiness Committee provides a senior representative to the command cell to make the decisions for their agency. This cell serves to improve and expedite

communication and coordination among the various members. The Captain of the Port is the lead representative of the committee. The MTMC Unit Commander assigned to that particular port represents MTMC interests. MTMC coordinates with the port manager, port police, local and state authorities, and the deploying unit commander to ensure the safety and security of personnel and equipment. The MTMC unit located at these ports is usually a Transportation Terminal Brigade (TTB), commanded by a Colonel/0-6. Each TTB has nine military police assigned, whose duties include coordinating with security forces of the deploying units, establishing security requirements for the safeguard of unit equipment, and establishing access control of personnel entering the port. Access is a key aspect of security. MTMC operations routinely make use of badge verification and escort systems to identify those individuals authorized to be in designated areas. The security element also makes recommendations regarding contracting additional security through the local economy.

Finally, as I mentioned previously, the execution of a deployment takes place quite deliberately at the port, from the arrival of unit equipment through the completion of offloading a vessel. Movement into and within deployment staging areas at ports is controlled at all times.

Procedures Instituted to Develop Risk Assessments for Strategic Seaports During a Mobilization

We have taken several steps to assess risks in Department of Defense strategic ports, and we are receiving assistance from many others to assess our strategic ports.

At the macro level, USTRANSCOM has instituted the Joint Risk Assessment Working Group (JRAWG) to provide operational risk management for all modes of defense transportation. This is a standing working group that reviews Transportation Component Command concerns that span the full spectrum of threat and force protection impacts to strategic mobility. The JRAWG makes risk

mitigation recommendations to the TRANSCOM operations division and command group when risk exceeds the operational need for mission support and/or force protection is assessed as inadequate. USTRANSCOM's intelligence directorate has activated an Asymmetric Threat Division, a collaborative effort of Counter-terrorism, Political-Military Affairs, and Information Operations analysts to produce and disseminate all-source threat analysis to USTRANSCOM assets and the Defense Transportation System (DTS). Additionally, USTRANSCOM has improved liaison with the FBI through a formal information-sharing relationship with the local field office in St. Louis and has formed a standing Joint Inter-Agency Coordination Group. Finally, a part-time FBI presence at USTRANSCOM and improved information sharing results in improved security and threat warning.

Prior to September 11th, we always included a terminal/port vulnerability determination in Annex B of our operations orders. We also conducted risk analyses for Army property as prescribed in Department of the Army pamphlet 190-51 and also took steps to identify any weaknesses. Defense Threat Reduction Agency (DTRA) conducted a Joint Staff Integrated Vulnerability Assessment (JSIVA) of the ammunition port at Sunny Point, NC, in June 2001. In August 2001, the Naval Facilities Engineering Service Center conducted red team assessments at our facilities at Sunny Point, NC, and Concord, CA. We then asked the Department of the Army G-3 (Operations) to visit Sunny Point and Concord in the Fall of '01 to further assess security and provide recommendations. They did so, and we have a program in place to acquire additional protective measures, many of which have already been accomplished. These enhancements are mentioned in the next section of my testimony.

We also benefit directly from risk assessments conducted during mobilizations. These include the conduct of security evaluations and vulnerability assessments of strategic seaports by the USCG, by the DTRA and the Joint Program Office, and by MSC. Certainly, the vulnerability assessments that Congress has recently requested the USCG to perform will enhance our ability

to do risk assessments of port operations. We will also couple those with specific intelligence reports we gather daily from our internal resources and commercial industry sources.

At the request of the U.S. Transportation Command, the DTRA and the Joint Program Office for Special Technology counter-measures have conducted vulnerability assessments of four of the strategic ports - Charleston, SC, Savannah, GA, Jacksonville, FL, and Beaumont, TX. The findings from the Charleston and Beaumont assessments have been provided to the Coast Guard's Captain of the Port (COTP) who will ultimately forward them to the appropriate port authorities. More are planned. USTRANSCOM's objective is to work with the Coast Guard to assess each of the strategic ports in rough order of their criticality with respect to the operations planning deployment support.

MSC also conducts individual risk assessments for port visits made by its vessels based on the threat level and Force Protection Condition in place at the time. This practice is mainly used when MSC vessels operate from overseas strategic seaports but has been and would be used as appropriate when MSC vessels operate using strategic seaports in CONUS.

Lastly, MTMC Commanders, acting as Port Managers for deployment operations, routinely use pre-deployment force protection checklists as a risk assessment tool. MTMC is going a step further to help determine security personnel requirements for specified strategic seaport operations. We are drafting a Port-Terminal Risk Analysis to be used for all deployments. It will take into consideration the criticality of the mission or operation, the location of the port, and sensitivity of materials being safeguarded. This analysis will define the adequate number of security personnel necessary to secure the port operation.

Changes Made Since September 11, 2001, Concerning How Security is Managed and Coordinated at Strategic Seaports During Mobilization of Military Forces and Cargo

A number of changes have been made as a result of the terrorist attacks. For example, before September 11, 2001, MTMC had no intelligence or counter-intelligence personnel directly assigned. However, the Army's Criminal Investigation Division (CID) provided a liaison agent to MTMC in October 2001 to provide direct intelligence support, which includes interaction with CID offices worldwide. This CID liaison has participated in eight port assessments to date and has been used in an advisory role by military forces moving personnel and equipment through the ports. Similarly, the Army's 902nd Military Intelligence (MI) Group has been actively engaged with MTMC and now provides support to us worldwide. USTRANSCOM's Counterintelligence Support Office maintains active contact with MTMC's Force Protection staff and provides counter terrorism support as required. USTRANSCOM also augmented MTMC with reserve intelligence officers at the onset of Operation ENDURING FREEDOM. These officers helped stand up a temporary G2 function. This temporary function is now being replaced by a permanent one in conjunction with Army Intelligence and Security Command. A Naval Criminal Investigative Service agent augmented Military Sealift Command, USTRANSCOM's sealift component.

As part of a major command restructuring, MTMC was moving to a split-based headquarters that would merge all operations, security management and intelligence at a single location in Ft. Eustis, VA, no later than June 2003. The events of September 11th and the ensuing operation - ENDURING FREEDOM - caused us to accelerate that process. A centralized operations center is now in place. The result has been positive for all facets of our traffic management and port operations missions. We now have a robust 24 hours a day/7 days a week operations center that is controlling deployments and other surface transportation worldwide from a single location. The new MTMC Operations Center, led by a one-star general, approves all port security planning and remains in constant communication with the geographic combatant commands we support, deploying units, commercial port and carrier industries, and the various

government organizations involved that have a coordinating role in the process. This capability has enabled us to exert positive control over port operations and react to any issues quickly and decisively. Additionally, the MTMC Operations Center receives and disseminates intelligence updates keyed to our operations worldwide.

While MTMC has limited organic security forces, the security forces at our disposal have successfully augmented our stepped up threat response. Currently, MTMC has three organic reserve Port Security Companies (PSC). One of the three PSC's has been activated since October 2001 and is assigned to the Military Ocean Terminal, Sunny Point, NC (MOTSU) - our largest ammunition port. The 4249th PSC is nearing the end of its one-year activation and will be replaced by the 1302nd PSC. The 4249th PSC has increased significantly the defense posture at MOTSU; and when personnel resources are available, they augment security for military operations at other strategic ports throughout CONUS. We are looking at the possibility of increasing the size of our PSC's and the number of security personnel assigned to our Transportation Terminal Brigades. The net result is an increased security presence for port operations.

In terms of heightened security at the two MTMC operated ammunition ports, the Military Ocean Terminal Sunny Point, NC, has improved its security posture by procuring a second security boat and towed sonar array system for waterside security, placing "Restricted Waterway" signs in the Intercoastal Waterway, improving landside perimeter security, and, as mentioned above, augmenting its DoD security force with a PSC. They are also receiving assistance from USCG Maritime Safety and Security Teams (MSST) during vessel operations. Future projects include construction of a waterside barrier system for three piers and an enhanced security perimeter system.

The Military Ocean Terminal Concord, CA, has improved its security posture by procuring two security boats for waterside security, receiving assistance from USCG MSST's during vessel

operation, installing a Vehicle Undercarriage Inspection System for vehicular traffic entering the port, and improving landside perimeter security. Future projects include construction of a waterside barrier system, posting restricted waterway signs in the water channel, and installing underwater detection capabilities.

How Will the Proposed Legislation, HR3983, and S1214, Assist in Coordinating the Multitude of Agencies Involved in Port Operations During Mobilization of Military Forces and Cargo?

We anticipate the proposed legislation will be very beneficial in a number of respects. We feel that the provisions directing DOT to assess the safety of all U.S. ports and to prepare anti-terrorism plans is critical and that the priority in sequencing those assessments be given to the 17 strategic seaports. As always, we will give our full cooperation to DOT and will share any assessments we have already completed to preclude redundancy or duplication of effort.

We agree with the need to have background checks and security identification issued by a central agency like DOT or the new Department of Homeland Security (DHS) depending on the final alignment of responsibilities. We have already heard from our commercial partners of the difficulty in trying to comply with a patchwork of identification requirements at the state, local, and individual port level. The National Defense Transportation Association, an agency that represents most of the commercial transportation businesses that deal in defense transportation, has included this requirement as one of the top ten initiatives it supports.

We obviously agree with the language that would have DOT or DHS establish teams to safeguard vessels, ports, facilities, etc. As I indicated earlier, MTMC does not possess significant organic resources to provide port security, and we rely on local port police, law enforcement, or contract security forces to fill in the gaps.

In a related vein, in August of 2001, the GAO began a comprehensive review of seaport force protection at those designated strategic seaports. The USTRANSCOM and MTMC hosted meetings with the GAO on this subject. The GAO also met with various members of the community involved with the security of Department personnel and cargo when moving through a strategic seaport. We have appreciated the careful, analytical, and cooperative approach of the GAO on this tough issue. While their final report has not been released, we suspect it will identify the complexity of seaport security and "who's in charge." As you have gleaned from my testimony, there are indeed many players - all trying to do their best.

Finally, we support measures that improve cargo identification and screening. While we move limited amounts of container cargo as part of unit deployments, we operate adjacent to commercial container operations at the seaports and we annually ship (primarily as exports) over 100,000 containers in commercial liner service to sustain our forces around the world. "What's in the box" is certainly one of the toughest challenges with which we all must deal in deterring terrorist acts.

SUMMARY

We are on the right path in the actions taken thus far to protect our personnel and cargo during deployment through seaports. The level of intelligence gathering, analysis, and sharing, along with the detailed preplanning for these events is unprecedented. The spirit of cooperation among all the players in the National Port Readiness Network structure is high. The evolution to standardized training across our worldwide port organization; the detailed risk assessments and force protection checklists; the attention to detail in the execution phase; and our robust 24 hours per day/7 days per week operations center have prepared us to operate effectively in this new environment. We are certainly not done. All agencies and departments involved in this process must continue to work together to continue

developing and implementing security measures to protect our valuable resources from ever-changing threats.

I am heartened that this committee is stepping out to address critical port security concerns on a national level. We owe it to the American public and our commercial transportation firms who need a single point of reference rather than a myriad of individual security requirements.

Mr. Chairman and members of the Committee, thank you for the opportunity to testify before you today.

Mr. PUTNAM. Captain Schubert, welcome to the committee.

Captain SCHUBERT. Good morning. Thank you, Mr. Chairman and members of the subcommittee. It is a pleasure to be here with you today to discuss the role of strategic commercial ports in homeland security.

The Maritime Administration plays an integral part in the deployment of U.S.-flagged vessels carrying military personnel and supplies to the theater. During a deployment, the Maritime Administration, also known as MARAD, serves to ensure that our commercial port facilities are available to the Department of Defense for military load-outs. In peacetime, MARAD acts as an advocate for our Nation's port community, which is a critical component of our economy.

The emergency operating arm of MARAD, the National Shipping Authority, is responsible for the acquisition and operation of ships for the defense service and for the coordination of shipping and U.S. commerce and the administration of the U.S. Government's war risk insurance program. Also, in the event of a national emergency, the National Shipping Authority administers a program to assure the priority use and allocation of commercial port facilities. If this authority is invoked, my responsibility is to serve as the director of the National Shipping Authority.

Coordinating port security during mobilization is not new to MARAD. It is an issue that we have been addressing for many years through the port readiness programs and the National Port Readiness Network.

The National Port Readiness Network has established Port Readiness Committees at each of our designated 13 strategic commercial ports. The local captain of the U.S. Coast Guard, Captain of the Port, are the chairpersons of those committees. MARAD chairs both the National Port Readiness Steering and Working Groups. These organizations provide coordination and cooperation to ensure readiness of commercial ports to support force deployment during contingencies and other defense emergencies.

To maintain heightened readiness and performance at strategic ports, MARAD assists its National Port Readiness Network partners in conducting port readiness assessments, monthly readiness status reports, mobilization planning, vulnerability assessments, and improving the deployment process. We have also partnered with the Defense Threat Reduction Agency and other groups in the development of risk assessments at our strategic ports.

MARAD is also concerned with port security because of its role in providing strategic sealift to the Department of Defense. Through the Voluntary Intermodal Sealift Agreement, also known as VISA, and the maritime security program, known as MSP, MARAD administers an emergency preparedness program that utilizes civilian transportation resources in a defense emergency.

MSP and VISA stem from DOT's authority under the Defense Production Act to prioritize sealift capacity for national defense purposes.

Since September 11th, a number of changes have occurred to improve port security. Obviously, port security is a major concern today, both in Congress and within the administration. Secretary Mineta has stated, "Protecting seaports and port facilities against

the threat of terrorism is imperative." The terrorist attacks have resulted in a renewed focus of security of our transportation systems, and we at the Department of Transportation are aggressively meeting these challenges on several fronts.

Congress is to be commended for its swift action in passing the Department of Defense Appropriations Act for fiscal year 2002, which included port security grant funding. From this supplemental appropriation, DOT was able to award 77 port security grants, totaling $92.3 million, including $38.1 million for our 13 strategic ports. That's roughly 41 percent of the total. These funds will be used to enhance facilities and operational security, provide for security assessments, and explore the use of new technology to improve maritime security.

As you know, port security legislation currently awaits action by the congressional conferees. Although neither bill has specifically addressed port security during a period of mobilization, the security measures that will flow from the passage of this legislation will certainly enhance security throughout the port system.

Since September 11th, MARAD has also focused on providing port security training and implementation of technology to improve security. In August of this year the U.S. Merchant Marine Academy's Global Maritime and Transportation School, which is administered by MARAD, will conduct security training for the State of Florida law enforcement officials.

On the international level, DOT and MARAD are working with the International Labor Organization, or ILO, to implement smart card technology to provide a reliable, secure mariner identification system in order to track employment records, minimize fraudulent documentation, and facilitate access to secure areas. A uniform and verifiable transportation worker identification card could facilitate the smooth flow of commerce and also promote security. Other technological innovations include cargo and container tracking systems and electronic container seals.

In conclusion, I have every confidence that the Port Readiness Network—this is due to my personal experience during Desert Storm/Desert Shield. In 1991, when I was based in Houston working for MARAD I was involved with the Port of Houston's day-to-day deployment activities. I can tell you we all pulled together. There was excellent cooperation between the Military Traffic Management Command, the Coast Guard and MARAD and State and local governments. We all knew our jobs and we did them well.

I would like to make a special mention that the Coast Guard performed an outstanding job in providing both shoreside and water-based force protection. We were able to secure our work area, credential dock workers, and load ships bound for the war zone without any serious disruption in commercial service. We were determined then and we are determined now.

I want to thank the chairman and members of this committee for the opportunity to address you here today, and I look forward to working with you on this vitally important issue in the future.

Mr. PUTNAM. Thank you, Captain.

[The prepared statement of Captain Schubert follows:]

DEPARTMENT OF TRANSPORTATION

STATEMENT OF

CAPTAIN WILLIAM G. SCHUBERT
MARITIME ADMINISTRATOR

BEFORE THE
HOUSE SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS
OF THE
COMMITTEE ON GOVERNMENT REFORM

July 23, 2002

Thank you, Mr. Chairman and Members of the Subcommittee, it is a pleasure to be here with you today to discuss the role of strategic commercial ports in Homeland Security. The Maritime Administration (MARAD) plays an integral part in the deployment of U.S. flagged vessels carrying military personnel and supplies; acts as an advocate for our Nation's port community; and serves to ensure that our commercial port facilities are available to the Department of Defense (DOD) in a national emergency. Secretary Mineta has said, "Protecting seaports and port facilities against the threat of terrorism is imperative. The terrorist attacks have resulted in a renewed focus on the security of our transportation systems and we at the Department of Transportation (DOT) are aggressively meeting these challenges on several fronts."

Effective port and intermodal security and readiness have become even more important since September 11th, and we are making it a priority to ensure a security-conscious environment at our 13 strategic port facilities. Commercial port security is critical to our future overall national security needs as the volume of international cargo and passengers continue to increase at our seaports.

The United States imports over six million containers annually. That figure is likely to grow dramatically in the next 20 years. The opportunity for security breaches in our active and increasingly congested national port system is unlimited. We must address security issues as a continuum that runs from awareness, to contingency planning, to prevention. By investing in technologies and capabilities that afford us greater understanding of the total maritime environment, we hope to predict security threats, take appropriate preventive measures, and protect our citizens and economic interests.

At the core of MARAD's mission is the promotion of U.S. shipping, shipbuilding, maritime labor and ports. But another equally important aspect of our mission is national security. We consistently work to reconcile our Nation's commercial maritime economic interests with its national security requirements.

DOT and MARAD are primarily responsible for the readiness of our strategic ports, and for establishing DOD's prioritized use of ports and related intermodal facilities during a mobilization. Without this intermodal and port infrastructure capacity and support, a seamless, time phased transition from peacetime to wartime operations cannot be adequately achieved. Port and intermodal facilities provide the critical interface between the water and surface modes of transportation, handling both commercial and military cargoes. With a reduced overseas presence, DOD must now rely more on commercial transportation resources located in the continental United States to deploy its forces. During military mobilizations, it is imperative that DOD be able to move war-fighting equipment and supplies through designated commercial port facilities quickly and securely to ensure optimal logistics flow to meet the mission requirements of overseas commanders.

The Maritime Administration provides the critical link between our vital commercial assets and our military complex. With our knowledge of the maritime industry, both ashore and afloat, we are able to effectively meet our defense requirements without adversely impacting our nation's economy. By design, the prioritization and allocation of commercial military assets is entrusted to a civilian agency.

Port Security Grants

Congress and the President are to be commended for their swift action in passing the Department of Defense Appropriations Act of Fiscal Year 2002 to include port security grant funding. The DOT, through MARAD, the Coast Guard, and the Transportation Security Administration, was able to award 77 port security grants totaling $92.3 million, including $38.1 million for our 13 Strategic Ports.

Port security grants totaling $78 million will fund enhanced facility and operational security. In addition, $5 million is provided for security assessments that will enable ports and terminals to evaluate vulnerabilities and identify mitigation strategies for their facilities, and $9.3 million will fund "proof-of-concept" projects, which will explore the use of new technology, such as electronic seals, vessel tracking, and electronic notification of vessel arrivals, to improve maritime security.

Port Readiness

Coordinating port security during mobilizations is not new to MARAD. It is an issue we have been addressing for many years through the Port Readiness Programs and the National Port Readiness Network (NPRN).

In 1984, a Memorandum of Understanding (MOU) established the National Port Readiness Network (NPRN). The NPRN is an organization made up of an executive level Steering Group, a staff level Working Group and local Port Readiness Committees (PRCs). The NPRN is comprised of MARAD, the U.S. Army Corp of Engineers, the U.S. Coast Guard (USCG), the Military Traffic Management Command, the Military Sealift Command, the United States Joint Forces Command, the United States Transportation Command (USTRANSCOM), the Maritime Defense Zone, and the U.S. Forces Command.

MARAD chairs both the National Port Readiness Steering and Working Groups. These organizations provide coordination and cooperation to ensure readiness of commercial ports to support force deployment during contingencies and other defense emergencies. Members of the NPRN Steering Group provide policy direction and set broad priorities for accomplishing the objectives set forth in the MOU. The Working Group is then responsible for implementing the policies and priorities set by the Steering Group. Overall, the Federal agencies and organizations who are party to the MOU have responsibility for support of the movement of military forces and supplies through U.S. ports in a national emergency.

The NPRN has also established PRCs at each of our designated 13 strategic commercial ports. The PRCs are chaired by the USCG Captain of the Port (COTP), and provide a mechanism to coordinate peacetime preparations for emergency port operations and for coordinating port operations during an actual national defense emergency.

The NPRN has been addressing port security concerns through national training workshops, PRC meetings, port readiness exercises (PRXs) and the use of the Incident Command System (ICS) during deployments. The ICS is a unified command structure that provides efficient coordination of port security during military deployments. The NPRN organization performed successfully during Desert Storm and Desert Shield. Last year, MARAD, in cooperation with the American Association of Port Authorities and the NRPN, sponsored a "National Strategic Commercial Port Workshop." Port and waterways security was specifically identified as a priority issue at this workshop.

MARAD also continues its outreach and training efforts in order to elevate the awareness of strategic port operations and port security. To maintain heightened readiness and performance at strategic ports, MARAD assisted its NPRN partners in conducting port readiness assessments, monthly readiness status reports, mobilization planning, vulnerability assessments, and improving the deployment process. We have also partnered with other agencies in the development of risk assessments at the strategic ports. For example, MARAD participated in the vulnerability assessments conducted by the Defense Threat Reduction Agency (DTRA) and the USCG at four strategic commercial ports. These assessments helped establish the methodology for future assessments.

MARAD, as part of its semi-annual port readiness assessment, also conducts a general assessment of port security, and has worked closely with USTRANSCOM on its Critical Infrastructure Protection Program.

Additionally, MARAD promotes port security through the Federal Port Controller Program. (The Federal Port Controllers (FPCs) represent MARAD in an emergency at the port level. FPCs are port executives who serve as MARAD's local agents and managers in emergencies. In peacetime, FPC designees represent MARAD on the local PRC.) MARAD fosters public and private partnerships with the maritime industry to provide adequate and timely access to commercial ports facilities and services for military deployment. Port Planning Orders and Allocation Orders are the instruments that assure DOD that adequate facilities and services are available to meet deployment requirements.

Maritime Security Program/Voluntary Intermodal Sealift Agreement

The Voluntary Intermodal Sealift Agreement (VISA) was established as an emergency preparedness program between the Department of Defense and Department of Transportation as the methodology for civilian transportation resources to be orderly managed and provided to support national security operations. VISA is an agreement that stems from the DOT's Defense Production Act (DPA) authority to prioritize and allocate dry cargo sealift capacity to national defense and economic requirements. MARAD's Maritime Security Program (MSP) is the primary vehicle that brings these civilian transportation resources into VISA, which include forty seven ocean-going ships, port intermodal management and services, and intermodal equipment such as containers and chassis. The Voluntary Tanker Agreement is a similar program administered by MARAD that provides tanker service/capacity for petroleum products. The combination of these programs provides for a seamless, time-phased transition from peacetime to wartime operations while balancing the commercial and defense elements of our maritime transportation industry.

DOD relies upon the DOT's authority to manage, prioritize, and allocate <u>all</u> civilian transportation resources to support both national and economic security during emergencies. The DOD has remained at arms-length from interceding in commercial economic transportation processes due to the separation between defense and civil agencies authorities and the fact that DOD's need for commercial transportation resources during an emergency occurs on a limited frequency. Drawing a parallel to military and economic cargo movement (... 95% by sea), the DOT's emergency preparedness program capacity and assets remain in commercial trade or "DOD stand-by" 95 to 99% of the time.

Ready Reserve Force

As part of our preparedness planning, MARAD maintains the National Defense Reserve Fleet (NDRF) and its Ready Reserve Force (RRF) component as a

source of additional cargo vessels in a national emergency. There are currently 41 militarily useful NDRF vessels moored at our three reserve fleet sites, and 73 RRF vessels located at 20 locations around the nation, excluding the three small RRF tankers outported in Japan.

MARAD maintains 51 RRF ships in four or five-day readiness status, providing them with permanently assigned Reduced Operating Status (ROS) crews for maintenance, and to facilitate activation. TRANSCOM provides general guidance for where they would like these ships to be located, and MARAD acquires berths in these areas such that the ships are within a short steaming distance from their expected load ports for defense cargoes. The berthing of ships in various ports around the country has the added benefit of avoiding congestion at the Reserve Fleet sites should a wide-spread activation occur.

National Shipping Authority

The National Shipping Authority (NSA) is the emergency operating arm of MARAD. It is responsible for the acquisition and operation of ships for defense service, for the coordination of shipping in U.S. commerce, the coordination of port services for defense and commerce, and the administration of the U.S. Government war risk insurance program. As the Maritime Administrator, I am also Director of the NSA. Selected MARAD officials are associated for planning with the principal NSA positions and take on the duties of those positions at the outset of an emergency.

In the interest of effective emergency use of ports, the NSA exercises certain controls over and coordinates operations of non-military ports in the United States and territories. In national emergency situations, the NSA administers a program to assure the allocation of priority use of commercial port facilities.

The Federal Port Controllers (FPC's) represent MARAD in an emergency at the port level. (FPC's are port executives who serve as MARAD's local agents and managers in emergencies). In peacetime, FPC designees represent MARAD on the local PRCs.

International Security Activities

Internationally, MARAD chairs the Organization of American States (OAS) Technical Advisory Group on Port Security, an industry and government partnership. Through this activity, we developed an Inter-American Port Security Training Program in which nearly 300 port personnel have been trained in the Western Hemisphere. This year, we will be conducting four training courses for our OAS trading partners. By improving the port security of our trading partners, we lessen the potential risks at home.

Port Conveyance Program

By delegated authority, MARAD conveys Base Realignment and Closures and other surplus Federal real property to public entities for the development or operation of a port facility. The program provides a no-cost means for local entities to acquire property for use as a port facility. The program helps create jobs and revitalize communities negatively impacted by base closures or other Federal action. However, the program also serves to ensure that property suitable for use as a port facility remains available for that purpose and for use by DOD if necessary.

To assist ports in expanding capacity to handle simultaneously both military and commercial traffic, MARAD has transferred over 2,000 acres of surplus Federal DOD property to non-Federal entities for port development. A prime example of this activity is the transfer of over 400 acres of Long Beach Naval property to the Ports of Los Angeles/Long Beach. The Port of Long Beach is one of nation's 13 Strategic Ports.

Port Security Legislation

As you know, port security legislation currently awaits action by Congressional conferees. Although neither bill specifically addresses port security during a period of mobilization, the broad range of security measures that will result from the passage of this legislation will certainly provide enhanced security throughout our port system, both for commercial and mobilization activities.

The Department supports the goals of H.R. 3983 and S. 1214, legislation that will heighten national awareness of the need for collective action and facilitate development of a coordinated interagency and public-private approach to port and waterways safety and security. The Department believes that a comprehensive approach to combating maritime terrorism is needed to assist in the prevention of, and to aid response to, criminal activity and terrorist attacks, and otherwise enhance port security by providing for port security threat assessments. It also supports an approach that will provide for the development of port security standards. The Administration also seeks a comprehensive, integrated approach to intermodal freight and cargo security.

The Department believes that a broad port vulnerability assessment program is critical to proper and efficient implementation of any port and maritime security and antiterrorism measures, both during peacetime and mobilization of troops and equipment. Because ports are varied in their size, layout, function and vulnerabilities, some sort of individualized assessment is necessary before any decisions can be made on what measures are necessary to protect any given port, including strategic ports. The Secretary of Transportation should also be allowed to establish standards for port vulnerability assessments, after consultation with public and private stakeholders.

The Department also believes that it is necessary to work with international organizations to develop standards and procedures for maritime security, and in consultation with the Secretary of State, undertake security assessments at foreign ports. The Department supports a comprehensive scheme for foreign port assessments, including the element of international operation and development of guidelines, which is crucial to the success of any effort to conduct assessments of foreign ports. For example, U.S. Customs' Container Security Initiative includes agreements with other countries to place U.S. customs officers in their ports for purposes of pre-screening containers destined to the United States. The initiative currently targets the "top 20 ports" in the world, in terms of cargo volume and participation is voluntary. Such pre-screening could facilitate the flow of cargo as well as promote security at strategic ports during a mobilization.

Center for the Commercial Deployment of Transportation Technologies (CCDoTT)

MARAD entered into cooperative agreements in FY 1997 with the TRANSCOM and California State University at Long Beach to assist in managing CCDoTT. The CCDoTT program demonstrates existing, emerging, and developing technologies in cargo handling, tagging, tracking, security, information management systems, and high-speed sealift.

These technologies, if adopted, will assist military deployment, improve port and intermodal security, expand the ability of commercial transportation to accommodate surge military cargo movements to minimize commercial transportation disruption.

Post 9/11 Activities

Since September 11, 2001, a number of changes have occurred to improve port security. The NPRN PRXs have more heavily focused on port security training and coordination. MARAD is also working closely with the Federal Highway Administration on convoy and port coordination and security to ensure a seamless secure transportation system between fort and port. The USCG is phasing in the use of the ICS during military deployments.

As stated earlier, MARAD has continued its outreach and training to elevate the awareness of, and emphasis on, strategic port operations and needs through a strategic commercial port workshop co-sponsored with the American Association of Port Authorities (AAPA). To maintain heightened readiness and performance at strategic ports, MARAD assisted its NPRN partners in conducting port readiness assessments, monthly readiness status reports, mobilization planning, vulnerability assessments, and improving the deployment process.

Additionally, MARAD has worked on the international and domestic level to develop Smart Card technology to provide a reliable secure transportation worker identification system, track employment records, minimize fraudulent documentation, and facilitate access to secured areas. A uniform and verifiable transportation worker identification card could facilitate the smooth flow of commerce, and also promote security.

Other technological innovations include cargo and container tracking systems and electronic container seals. We are also pursuing, through our lead cooperative programs, the Ship Operations Cooperative Program and the Cargo Handling Cooperative Program, the development of answers to pressing technology and practice issues to assure that the most appropriate technological solutions and approaches to the problems we collectively must solve.

Summary

Ironically, on September 11th of last year, MARAD was hosting the National Strategic Commercial Port Workshop when the terrorist attacks occurred. The participants of the meeting that day instinctively understood the important role the nation's port community would play in this new struggle against terrorism. The maritime industry's contribution to the nation's economic and security needs is well documented. Never before, however, have I seen such a sense of determination and single mindedness in this community to succeed over an adversary. I want to help build on that sense of determination to meet the joint challenge of economic and homeland security.

I actually experienced this determination and single mindedness first hand in the Desert Storm/Desert Shield conflict. In 1991, when I was based in Houston working for MARAD, I was involved in the Port of Houston's day-to-day deployment activities. I can tell you, we all pulled together. There was excellent cooperation between Military Traffic Management Command, the Coast Guard and MARAD. We all knew our jobs and we did them well. We were able to secure our work area, credential dockworkers and load ships bound for the war zone without any serious disruption in commercial service.

I want to thank the Chairman and the Members of this Committee for the opportunity to address you today. I look forward to working with you on this vitally important issue in the future.

This concludes my prepared statement. I would be pleased to answer any questions you may have at this time.

##

Mr. PUTNAM. At this time the Chair recognizes Admiral Pluta. Welcome to the subcommittee.

Admiral PLUTA. Thank you, Mr. Chairman. Good morning, Mr. Chairman and distinguished members of the committee. I appreciate the opportunity to be here today to discuss the Coast Guard's efforts in protecting our Nation's strategic seaports. The Coast Guard, with primary authority from the Espionage Act of 1917, and the Magnuson Act of 1950, is the lead Federal agency for reducing, preempting, deterring, and defending against security threats targeting ports, waterways, and the coastal areas of the United States and its territories.

As a unique instrument of national security, the Coast Guard is the only military service with civil law enforcement authority, regulatory and safety responsibilities, and Captain of the Port authorities. These authorities prompted a memorandum of agreement signed in 1995 by the Secretaries of Transportation and Defense, the Chief of Naval Operations, and the Commandant of the U.S. Coast Guard to provide interdepartmental recognition of Coast Guard capabilities in support of the national military strategy. The memorandum of agreement establishes port operations, security, and defense as a mission of the Coast Guard, including the use of Coast Guard forces to help provide anti-terrorism force protection from military forces in the United States and overseas.

It is through a well-defined command and control structure at the local level and strong partnerships with key public and private port stakeholders that the Coast Guard is able to accomplish these missions. Guided by the National Port Readiness Network, the Captain of the Port is the lead agency responsible for coordinating Federal, State, and local resources, as well as private entities in the port region, in executing port security responsibilities during any mobilization or national defense contingency operation. This is accomplished primarily through port readiness, harbor safety, and port security committees at the local level.

As a former Captain of the Port for the strategic ports of Wilmington, North Carolina; Morehead City, North Carolina; and Southport, North Carolina, I can't emphasize enough the importance of a coordinated approach by all maritime players in carrying out this critical function of port security, especially as the United States continues its overseas military operations.

Additionally, the Captain of the Port could receive significant assistance through the passage of pending comprehensive port security legislation currently being reviewed in conference. Through a well-developed hierarchy of port security plans, Federal, State, and local security activities and resources will be more effectively aligned in addressing our collective homeland security responsibilities.

The Coast Guard has been working closely with the Transportation Command, the Military Sealift Command, the Military Traffic Management Command, Department of Navy, and the Maritime Administration to identify gaps, validate security requirements, and establish a scheduling process for coordinating Coast Guard waterside security during priority outlooks.

Another key initiative in closing security gaps has been the increased emphasis on vulnerability assessments for U.S. seaports.

Even before the events of September 11th, the Coast Guard was actively working with DOD on their methodology for identifying port vulnerabilities in strategic seaports.

Although the principles of port security for strategic seaports are built around the prevention of a terrorist event, safeguarding our strategic seaports against a broad spectrum of threats requires a comprehensive maritime domain awareness. A robust maritime domain awareness will provide all leaders with the knowledge base needed to frame the optimum policies, decisions, and operations to protect our strategic seaports.

The importance of protecting and supporting the movement of military forces and supplies through U.S. seaports is never more critical than it is today. Protecting military load-outs in the continental United States and its territories is a longstanding mission of the Coast Guard that requires a well-coordinated effort with our Government and industry partners. It is incumbent upon our Government agencies and military services to balance the resources and meet the challenge of protecting our critical military assets and infrastructure.

Thank you for the opportunity to testify before you today. I will be happy to answer any questions that you might have.

Thank you, Mr. Chairman.

Mr. PUTNAM. You're very welcome, Admiral.

[The prepared statement of Admiral Pluta follows:]

DEPARTMENT OF TRANSPORTATION
UNITED STATES COAST GUARD
STATEMENT OF REAR ADMIRAL PAUL J PLUTA
ON
HOMELAND SECURITY: PROTECTING STRATEGIC PORTS
BEFORE THE
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS
COMMITTEE ON GOVERNMENT REFORM
U. S. HOUSE OF REPRESENTATIVES
JULY 23, 2002

Good afternoon Mr. Chairman and distinguished members of the Committee. I appreciate the opportunity to be here today to discuss the Coast Guard's efforts in protecting our nation's strategic seaports from terrorist attacks in the wake of September 11th.

The Coast Guard is the lead federal agency for reducing, preempting, deterring and defending against security threats targeting ports, waterways and the coastal areas of the United States and its territories. The Espionage Act of 1917 and the Magnuson Act of 1950 provide the Coast Guard with the authority to safeguard all vessels, ports and facilities from acts of sabotage or other subversive acts. As a unique instrument of national security, the Coast Guard is the only military service with civil law enforcement authority, regulatory and safety responsibilities, and Captain of the Port authorities.

These unique authorities prompted a Memorandum of Agreement (MOA) signed in 1995, by the Secretaries of Transportation and Defense, the Chief of Naval Operations, and the Commandant of the Coast Guard, to provide inter-departmental recognition of the use of Coast Guard capabilities in support of the National Military Strategy. This important MOA establishes Port Operations, Security and Defense as a mission of the Coast Guard. This mission includes the use of Coast Guard forces to provide antiterrorism /force protection (AT/FP) for military forces in the United States and overseas. Thus, the Coast Guard is primarily responsible for ensuring the U.S. Marine Transportation System and its major shipping channels are open and marked, and that military transport ships are provided safe and secure passage from U.S. harbors to open ocean.

It is through a well-defined command and control structure consisting of the Coast Guard Captains of the Port (COTP's) and Group Commanders that the Coast Guard is able to accomplish these missions and provide a blanket of protection. However, in addition to its own resources, the Coast Guard depends heavily on its many Federal, State and local partners who have a significant stake in maximizing the protection of maritime infrastructure and military outloads in U.S. Strategic Seaports. Guided by the National Port Readiness Network (NPRN) as set forth in the 1985 and recently revised Port Readiness Memorandum of Understanding between the Departments of Transportation and Defense, the Captain of the Port is the lead agency responsible for coordinating federal, state, local resources and private entities in the port region for executing AT/FP responsibilities during any mobilization or national defense contingency operation. This is accomplished primarily

through port readiness, harbor safety, and port security committees at the local level. The Captains' of the Port coordination function would receive a significant boost through the passage of the comprehensive port security legislation currently in conference. With a well developed hierarchy of port security plans, federal, state and local security activities and resources will be more effectively aligned in addressing AT/FP responsibilities and overall Homeland Security. The Coast Guard's integral partners and force providers in carrying out its security role, include but are not limited to the Department of Defense, Department of Justice (FBI, INS, DEA), Department of State, Office of Homeland Security, Department of Agriculture, U.S. Customs, Office of National Drug Control Policy, Military Sealift Command, Military Traffic Management Command, Federal Emergency Management Agency, the Environmental Protection Agency, the Maritime Administration, the intelligence community, and the maritime industry.

During times of war or national emergency and to protect against asymmetric and terrorist threats, two Maritime Defense Zone (MARDEZ) Commanders are assigned, each with a robust command structure and access to a wide variety of Navy and Coast Guard capabilities. Maritime Defense Zones are Navy commands responsible to their respective fleet Commanders for Naval Coastal Warfare and are headed by Coast Guard Atlantic and Pacific Area Commanders. MARDEZ Commanders are responsible for deploying forces to conduct Coastal Security, Port Security, and Harbor Defense operations along the U.S. coast. Coast Guard and other military forces and government agencies available to carry out these missions are equipped with patrol craft, cutters, and aircraft. An additional capability will be provided by the new Maritime Safety and Security Teams (MSSTs), a deployable force with AT/FP expertise currently being stood-up in a number of locations throughout the country. The Department of the Navy and the Coast Guard are also partnering through the Navy/Coast Guard (NAVGARD) Board. Coast Guard and Navy AT/FP working groups led by Area/Fleet Commanders have promulgated interservice guidance on Coast Guard support to Navy ships

In support of the MARDEZ Commanders, the Naval Coastal Warfare (NCW) program provides a joint force package that provides a layered defense for port operations and security. The program is currently staffed by active and reserve Navy and Coast Guard personnel in leadership and operational positions within the NCW Program. In the aftermath of the attack on USS COLE and particularly post-11 September, the role, structure, and utilization for the NCW program has changed and continues to evolve with developing world events. NCW Groups and Units and Coast Guard Port Security Units have been mobilized to perform force protection missions at different levels in all combatant commanders' areas-of-responsibility and within the continental United States in support of Maritime Homeland Security.

The attacks of September 11th and on the USS Cole, while not changing the authority of the Coast Guard, have required a new look at clearly delineating security responsibilities during military loadouts. AT/FP requirements have expanded from a reserve-centered contingency support model to a more constant presence supporting the movement of all military resources from domestic Seaports of Embarkation. This is a far more resource intensive effort. In an effort to close gaps that might exist, the Coast Guard has been working closely

with the Transportation Command (TRANSCOM), Military Sealift Command (MSC) and Military Traffic Management Command (MTMC), to validate security requirements and establish a scheduling process for coordinating Coast Guard waterside security during hazardous materials, explosives, and military equipment outloads. The new MSST's will provide additional resources for security activities during military loadouts.

A key initiative in closing security gaps has been the completion of Port Security Assessments (PSA's) in several strategic U.S. seaports. These PSA's were conducted by TRANSCOM's Critical Infrastructure Protection (CIP) Group through a partnership with the Coast Guard and DoD's Defense Threat Reduction Agency. Since last fall, assessments in Baltimore, Guam, Honolulu, Charleston, and Savannah were conducted and are the foundation for the broader Coast Guard PSA program underway in additional seaports throughout the country. Under the PSA program, militarily strategic ports will be given priority. The PSA is a comprehensive analysis of U.S. seaports to make federal, state, and local governmental agencies and other appropriate port stakeholders aware of the susceptibility of maritime critical infrastructure to negative consequences from intentional acts of terrorism. Based on the results of the assessment mitigation strategies are then recommended to the local maritime community for further action to protect the public, the environment, and U.S. economic interests as required for national security.

As we move forward, we must change our approach to seaport security. Although the principles of AT/FP for strategic seaports are built around the prevention of a terrorist event, it is the element of awareness of the potential threats around us that is key in helping focus limited resources on prevention. Safeguarding our strategic ports against a broad spectrum of threats requires comprehensive Maritime Domain Awareness (MDA). Essentially, a robust MDA will provide national leaders, operational commanders, and maritime stakeholders the knowledge base needed to frame the optimum policies, decisions, and operations that will protect strategic seaports. Ultimately, the success of MDA will depend on unprecedented information and intelligence sharing among federal, state and local agencies, international partners, industry, non-governmental organizations, and citizens.

In summary, the importance of protecting and supporting the movement of military forces and supplies through U.S. Seaports is never more critical than it is today. Protecting military loadouts in the Continental U.S. and its territories is a longstanding mission of the Coast Guard that requires a well-coordinated effort with our government and industry partners. Ultimately it is incumbent upon our government agencies and military services to balance the resources and meet the challenge of protecting our critical military assets and infrastructure. Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

Mr. PUTNAM. We appreciate the entire panel being here and we thank you for your thoughtful opening statements.

We have a journal vote pending, so the subcommittee will stand in recess for a few moments. We will be back as soon as possible. Subcommittee stands in recess.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene. My apologies to the panel. Our logistics command here in Congress also has some systemic problems.

At this time I would like to recognize Mr. Schrock for any questions that he may have.

Mr. SCHROCK. Thank you, Mr. Chairman.

I'm going to emphasize again how important this issue is to me. I'm sorry there aren't more Members here because the bad guys got us one way before, and I think the next way they are going to do it is by sea. I don't like to scream "fire" in a crowded theater and I'm not Chicken Little with "the sky is falling," but, by golly, if we don't address this thing we're going to have another September 11th and it is going to be in the waters of America. We just have to prevent that.

This is a broad question, General, but you talked about cargo and identification screening. I'm just trying to figure out how we solve that. I hear a lot of people say, "We need to make sure when the container ships come to our shores, when they are off-loaded they are checked." I'm here to tell you that's too late. If a ship leaves Alexandria, Egypt, with a little weapon on it and it gets behind our carrier piers in Norfolk, for instance, and GPS system sets it off, it is too late. But how do we do that? I know that's a terrible question to ask, but I try to think of that all the time and don't know how to do it unless you get all these other countries to agree to do something like that. But how do we do that?

General PRIVRATSKY. Sir, I don't think there is a single answer to how you do that. I don't think that you can check containers adequately at either end of the supply chain and make it effective. I think, as we work toward the best solutions, we are going to find ourselves leveraging our robust technology capabilities, analyzing patterns, analyzing shippers, analyzing cargo, analyzing discrepancies related to all of that, to use technology to try to identify what we then see as being particularly risky, and then applying our cargo screening toward that.

I do not see a future where we will ever be able to screen all cargo at either end, or we're going to bring supply chains to their knees.

Mr. SCHROCK. It would certainly impact commerce. Admiral.

Admiral PLUTA. Thank you, sir. I thought it would be worth mentioning, the concepts behind the approach we are taking in concert with all the agencies involved with this challenge, and I think it is the biggest challenge that we face in the security realm, the cargo security part, particularly containerized cargo.

The solution set that we are focusing on is end-to-end cargo integrity from the point that the box is loaded to the point that it arrives at its destination, and that includes having a trusted agent at the loading, having a higher, sophisticated kind of locking system and better containers that can be interrogated electronically,

and have a chain of custody as it moves along all the way from its point of loading to the point of destination—a lot of information sharing that needs to be done, manifesting, proper manifesting of the cargo.

What helps that is that we are putting into place security requirements, both domestically and internationally, for people to do cargo security, in particular, better so that we can recognize those companies that do security well, have solid security plans in place, and do vet them and audit them properly, and those people can—we don't need to waste our time looking at people who do security well. We can focus on those that we know less about. And so it is an incentive program that will help us get that job done because of the millions of containers that come into our ports. It is a very difficult problem.

Mr. SCHROCK. I think I heard there were 16,000 containers offloaded in America every single day. That's a lot.

Admiral, let me followup with you. First of all, let me tell you how wonderful I think the Coast Guard is. I mean, their mission has not been fully appreciated over the years, and I think now we certainly understand how important the future role of the Coast Guard is going to be—and that's from a guy who wore the Navy uniform for 24 years. You're part of our sea services, and I'm really proud of what you do. And I want to make sure, if Congress isn't giving you what you need, keep coming back and screaming. Jim Loy, Admiral Loy, former commandant, was the first head of the services who had the courage to stand up and say, "Congress, enough is enough. Unless you give us the funding to do what we need, we can't do any more." I thought that took a lot of courage, and the others fell in line behind him.

You talk about a coordinated approach. I had a working group over in Anacostia, I believe it was—over in Suitland several months ago, and had 15 Government agencies there. What I found was, you know, I think interoperability, keeping agencies being able to talk to one another is very important in sharing information, but what I found was that a lot of the agencies would love to share some of that information but by law they can't, which just makes absolutely no sense to me. Are you finding that the case? How do we break that down? I guess it's going to have to come from here, most of it, to pass laws to get rid of laws so you all can talk to one another. Has that been a problem for you all?

Admiral PLUTA. Yes, sir, it has been a big challenge. Ever since the President's Commission on Critical Infrastructure Protection, we recognized that there would be difficulty sharing classified threat information with the people who actually own the infrastructure—in large measure, the private sector. So the concept that the Presidential decision directors put in place was ISACs, they call them—Information Sharing and Analysis Centers—so that the FBI, when they get credible threat information, can share them through the ISAC right directly to the people who need it.

As we speak, Coast Guard people, FBI people, people from the maritime community are putting together an Information Sharing and Analysis Center for the maritime mode to get that threat information and be able to share it widely. The challenge will be to get

the security clearances to the people who ultimately need that classified information.

Thank you, sir.

Mr. SCHROCK. All right. That's good news.

Let me just ask one more question, Mr. Chairman, and then I will keep quiet.

Captain, you talked about security assessments, you all were doing security assessments. I guess that's a follow-on to what I asked the admiral. Are you able to do those in conjunction with other agencies, or are there stumbling blocks, roadblocks in the way that prevent you from doing that?

Captain SCHUBERT. The security assessments—there's really on two fronts that's being done. The Coast Guard is—and Admiral Pluta could address this I more detail—is developing a standard to do what we call "port security assessments." These are very comprehensive assessments, and there have been some that have been done. At least two of the thirteen commercial strategic ports have been completed, and there are plans ahead to do the rest of them.

The other security assessments when we talk about it was through the port grants that we just—that I just mentioned earlier in my opening statement. We have funded out—of the $92.3 million, approximately $5 million of that went to help ports do their own security assessments, and approximately $633,000 of that were security assessments to help fund the ports in the 13 strategic ports that had requested money to do that. So that's really where we are.

Admiral, did you want to add anything?

Admiral PLUTA. Sir, the port vulnerability or port security assessments, we're planning on hitting all 55 of the strategic and economical ports in the United States over the next 3 years. It is resource-constrained evolution. We hope to get eight accomplished this year, and we will have all the strategic ports front loaded in that because we weighed heavily in that direction.

Thank you, sir.

Mr. SCHROCK. Well, thank you to all. Just know that if there is any way I can carry your water and help you with this, I'm here all the time to help you with that, and I'm not kidding. It is a huge issue for me, and I want to help you in any way I can.

Mr. PUTNAM. Thank you, Mr. Schrock.

We'll note for the record that Mr. Allen and Ms. Watson have arrived. At this time, the Chair recognizes Mr. Allen for 7 minutes.

Mr. ALLEN. Thank you, Mr. Chairman. I may not need all of that.

I apologize for not being here for your testimony.

The port in my District, Portland, Maine, is probably not going to have a lot of troops moving through it, but I do want to ask you, Admiral Pluta, about the Coast Guard's general role with respect to ports—port security. I'm thinking, of course, of my own. In particular, to what extent is the Coast Guard working to develop affiliations with others who are using the ports in the ports available to keep their eyes and ear open?

By way of background, just to give you sort of the setting for my question, I was touring. I went out in the harbor, the Portland Harbor, the other day with the waterfront director and a variety of

other people. It is clear that what we're trying to do there is, from the local fire fighters on the fire boat, to the Coast Guard, to the fishermen, to all the others who are out there using the port, there is a sense that we need to use all of the people who are using the port for other reasons and tie them together somehow to be the eyes and ears in order to protect the area. That's separate from the whole issue of commercial transportation and containers and so on.

But I wondered at your level whether you're giving some thought to that issue and how you are approaching it.

Admiral PLUTA. Thank you, sir.

The answer to your question is yes, absolutely. We have been working that issue since September 11th. In particular, up in your area the First District commander, Admiral Cray, is working with the fisheries community. I can't remember the specific name of the program, but it is—Coast Watch is the name of the program. In particular, working with the fishermen, telling them specifically what sorts of suspicious things we might be interested in hearing and who to contact—"Here's the telephone number, here's the contact point."

We have worked not only that up in your area but around the country. On the national level, we've entered into memorandum of agreement with the American Pilots Association. In large measure, the pilots are the first Americans that set foot on a foreign-flagged vessel when they come into the United States. Also, the National Cargo Bureau, which is the first view of cargo that comes into our country. And we published an 800 number, our own 7-by–24 national response center for people to call in for any suspicious activity. We have Port Readiness Committees at every port around the country, including Portland, where all of the port stakeholders come together to discuss security issues.

So we have tried to—we know that we don't have enough resources to do this job ourselves, sir, and so we have reached out in large measure to try to help expand our forces.

Mr. ALLEN. One more question. Again, it is not the precise subject of this hearing, but I have been told that the resources of the Coast Guard after September 11th have been diverted really to protecting the homeland, and, of course, up and down the Maine coast the search and rescue function, the sort of watching out for fishing vessels and just being available for all of those other tasks has been a real concern. How are you now trying to balance your different roles and functions, the ones you were focused on before September 11th and the new significance of homeland security? How are you sort of not giving up the old to take on the new?

Admiral PLUTA. Thank you for that question, sir. It is very important to us because we consider that everything we do plays a role in national security one way or the other. The security of our citizens is equally as important in their day-to-day safety, life at sea, as it in the anti-terrorism context. So, in simple answer to your question, right after September 11th, because no one in the country knew what to expect next, we diverted all of our assets to defending our ports, and we spent up to—about 58 percent of our operating expenses of our budget were directed at maritime security.

We recognized we couldn't sustain that. We needed to get back to fisheries patrol, search and rescue, drug enforcement, migrant interdiction, and so over time we migrated those larger assets back to those missions, and what the Commandant of the Coast Guard established is a multi-year strategy to get us sufficient resources to do all of those things.

We're starting to commission maritime safety and security teams—there will be six of them scattered around the country initially—so that they could be our domestic surge capability should another terrorist event occur so that we wouldn't have to divert search and rescue and law enforcement assets to do that job.

But we haven't degraded our capability. We are back to not full capacity but near full capacity in those missions, and we are working over the multi-year strategy with your help, sir, to get back to the point where we can do both for the country.

Mr. ALLEN. Admiral, thank you very much. Thank you, Mr. Chairman.

Mr. PUTNAM. You're very welcome. And we'll note for the record that Mr. Tierney from Massachusetts has joined us, and the Chair recognizes the chairman of the subcommittee, Mr. Shays.

Mr. SHAYS. I thank you, Mr. Chairman.

Admiral Pluta, I was not being facetious when I was saying hopefully you will find yourself under not the Department of Transportation but the Department of Homeland Security. I am intrigued by the sense that I get from your testimony that you all feel that coordination is pretty good. Is that an accurate statement among all three?

Admiral PLUTA. Not perfect, Mr. Chairman, but certainly better than it ever has been.

Mr. SHAYS. And, Captain, you nodded your heard, so that's a yes?

Captain SCHUBERT. Yes, I agree with that. Not perfect, but we do work well together. And I think what is most important is when the balloon went up for the Gulf War, that should be one of the best examples of how we can really work together, and we did work together very well.

Mr. SHAYS. General.

General PRIVRATSKY. Sir, I am cautiously optimistic. There is no question that since September 11th that our focus has shifted more to security than readiness in port operations, and our Port Readiness Committees by name are becoming more and more Port Security Committees because of that shift in emphasis. In September we just did not view the threats to our homeland as we view them today, and so there has definitely been a migration of focus toward more security.

Mr. SHAYS. Let me make reference to the GAO, who will testify later today. They said, "Uncertainties regarding the seaport security environment exist because comprehensive assessments of threat, vulnerability, and critical port infrastructure functions have not been completed and there's no effective mechanism to coordinate and disseminate threat information at the seaports."

Should I read it again, or did you all hear it? I'd like you to respond to that. Why don't we start with you, General?

General PRIVRATSKY. In terms of risk assessments, we have had a very systematic number of assessments for ports underway over the past several years. Specifically, if we looked at one of the ports that garners a lot of my attention, our ammunition port at Sunny Point, we had two——

Mr. SHAYS. I'm sorry. Sunny Point is which State?

General PRIVRATSKY. North Carolina.

Mr. SHAYS. Thank you.

General PRIVRATSKY. It's our high-volume ammunition port. We had two threat assessments at that port pre-September 11th and after September 11th we had another one conducted by Department of Army, and we have implemented recommendations from those.

U.S. Transportation Command has requested the Defense Threat Reduction Agency assessment of strategic ports. Four have been conducted to date. Others will follow.

And so I think that there is a thorough assessment. I know at that ammunition port I mentioned that we have taken very deliberate action after those assessments and we're a lot different now than we were in September and we'll be different in the future.

Mr. SHAYS. Before I leave you, General, let me ask you, you responded to the threat assessment. The second part of that comment was that critical port infrastructure functions have not been completed and there's no effective method to coordinate and disseminate threat information at the seaport. Take that point about infrastructure not being completed.

General PRIVRATSKY. Well, we have an integrated priority list of projects that is managed by the U.S. Transportation Command to resource fixes toward strategic ports. I can provide a more-detailed answer for the record for you on that.

Mr. SHAYS. Let me just stick with you again, General, to say in the report from GAO they say, "We identified two significant weaknesses associated with DOD's force protection process for deployments through domestic seaports. First, DOD lacks a central authority responsible for overseeing, coordinating, and executing force protection measures while military forces deploy from domestic installations through U.S. seaports." Can you respond to that?

General PRIVRATSKY. There is no centralized DOD authority for controlling that, but port security falls underneath the Coast Guard, and that at a local level comes together at the Port Readiness Committees, of which my command plays routinely.

Mr. SHAYS. Let me just jump then to the Coast Guard. I've always gotten the feeling that the Department of Transportation considers the Coast Guard somewhat of a step-child, with no disrespect to step-children, but, frankly, it hasn't been funded properly by Congress. I think we all know that and we've known it for a number of years.

I'll leave with that negative note and I'll come back for a second round, Mr. Chairman. My time is up.

Mr. PUTNAM. Thank you, Mr. Chairman.

The Chair recognizes Mr. Watson from California. Mr. Watson, do you have questions?

Ms. WATSON. Thank you, Mr. Chairman, and thank you, gentlemen, for being here.

I have a District that once included the coastline of Southern California. However, most of our military transportation and so on, our military transferrals, are out of the, I think, Stockton Harbor. Maybe some of you are aware.

My question to anyone who can respond is: how far out does the line go? Is there a possibility that the enemy could be within, say, a 20-mile radius, a 30-mile radius, and still do damage to us? Do we scout out beyond that line for any kind of craft that might have mal-intent? Can you just respond in general, please?

Admiral PLUTA. Thank you, Ms. Watson. Yes, we have jurisdiction. The Coast Guard has jurisdiction out to the 200-mile exclusive economic zone of our country.

Ms. WATSON. 200 miles.

Admiral PLUTA. We're working on, with Congress' help, enabling legislation for us to require automatic identification systems for vessels. They will all be required to carry transponders which transmit information about their name, their flag, last port of call, things such as that.

We also, because the bad guys will turn it off, we also are working with the Department of Defense on surveillance systems so that we can cross-check the responder information and be able to tell the legitimate traffic from those that may not be. And so we do have the jurisdiction, we exercise the jurisdiction. We identify 96 hours before a vessel is scheduled to arrive at the United States. We will identify whether or not they have any suspicious crew members or any problems with their cargo, and we will keep them out of port and board them with a multi-agency boarding off-shore before we'll ever let them in port if we suspect that there might be something amiss.

So it's not just a port-related focus, although that's very important. We're also concerned about the maritime domain awareness of knowing which vessels, which cargo, which people are coming in the direction of the United States.

Ms. WATSON. Let me go back to a little history. We were all stunned by the "U.S.S. Cole" incident. As I understand, that was supposed to be a craft bringing food to the ship?

Admiral PLUTA. I'm not familiar specifically. I thought it might have been an anchor-handling vessel or an anchor-handling crew that they thought it was or could have been bringing food. In any case, we are concerned about a Cole-type event, and particularly working with the U.S. Navy. That's why we identify vessels of high interest, and if we suspect that there might be a crew member who has a suspect background, we will put Coast Guard people on board as that vessel transits in, and we'll put Coast Guard vessels alongside to escort it if it is a high-consequence vessel like a Navy vessel or a cruise ship or something like that, so that our escort vessel will be able to shoulder away any small boat that may want to come by.

In the case of Naval vessels, we'll establish a Naval vessel protection zone around their assets, and by law people that enter that zone will be violating the law and we can enforce that against them.

So yes, we factor in Cole-type incidents. We don't have enough assets currently, but with our multi-year budget strategy and with

what is coming into the Coast Guard and what's coming into the Department of Defense, we will be able to deal with that threat, as well.

Ms. WATSON. Being a late arrival—and I apologize for that—you might have mentioned this, but have you graded and rated the ports as to their vulnerability, as to those who are at higher risk? And, if so, is there a list available?

Admiral PLUTA. Yes, ma'am. There is a list of strategically and economically important ports to the United States that the Department of Transportation has focused on in cooperation with the Department of Defense, and so we are focusing our attention on those 55 of the 361 ports in the United States first.

Ms. WATSON. Are they ranked?

Admiral PLUTA. Yes, ma'am. It's a classified document and we can provide that to you in a separate forum.

Ms. WATSON. Yes. I just want to know how many are on the west coast, California, if somebody could get that to me.

Admiral PLUTA. Could we get back to you off-line on that, ma'am?

Ms. WATSON. Yes. I just want to add that right after September 11th we did hold a forum out in California in Los Angeles about preparedness and readiness across the board, and our big concern was about our Port of Los Angeles, but troop movement usually is out of, as I said, the Stockton area, the North Bay area.

I must commend them for, you know, the constant vigilance. I would just like to know are we up to par, have we done all that we can do, and what kind of risks or vulnerability do we face. So if you could get that information to me I can join with my colleagues from California to be sure that we see that our various military units and those people responsible are keeping at this in securing. I'd appreciate that information.

Admiral PLUTA. Thank you, Ms. Watson. We will provide you with that list, and with your help over time I think we'll get to where we need to be to provide all the protection your ports deserve.

Ms. WATSON. We're there.

Admiral PLUTA. Thank you.

Ms. WATSON. Thank you.

Mr. PUTNAM. Thank you, Ms. Watson.

Ms. WATSON. Thank you.

Mr. PUTNAM. Captain Schubert, as the maritime administrator, you are also director of the National Shipping Authority, and that position is only mobilized in times of emergency; is that correct?

Captain SCHUBERT. That's correct. The President needs to invoke a national emergency or war.

Mr. PUTNAM. And when was the last time that was mobilized, that occurred?

Captain SCHUBERT. It is kind of interesting. During Desert Storm—the last time it was evoked was probably—I'd have to get back to you on exact answer, but I want to reflect back to Desert Storm/Desert Shield. During that mobilization we acted under the National Port Readiness Network as if it was invoked, and we actually did issue one priority order to a ship yard under that authority. So I would say that was probably the last time it was invoked,

because we did invoke or issue a priority order to utilize commercial facilities, and it was done once during that engagement.

Mr. PUTNAM. So it is—but even in that situation it wasn't really fully engaged. It was used in that instance; is that a fair characterization?

Captain SCHUBERT. Yes, and there's an interesting reason why it wasn't fully engaged. Again, I'll relate to the Port of Houston, which was the second-largest load-out port. In that instance, the MTMC and MARAD worked very closely together as to what the requirements are.

Our role is to make sure that, when we go in and prioritize and allocate public resources, that it does not disrupt commerce to—has the least impact on the disruption of normal flow of commerce.

In this case, in Houston we were able to negotiate with the Port of Houston to use one berth, basically one berth that they had as a primary load-out without disrupting the commercial flow, so we were able to do that without actually issuing what we call a "port planning order." That was modeled pretty much throughout the United States.

Mr. PUTNAM. Does it concern you that in time of war the plans that are in place for a war or for a national emergency were not fully engaged, which begs the question of whether we have the right plans in place? And, second, that we were essentially responding to the war effort in a logistics capacity by doing what was most convenient for commercial shippers?

Captain SCHUBERT. No, that didn't concern me on either count. We weren't just doing—first of all, to answer the last part of your question, we weren't just concerned about commercial shippers, but that is the reason why, under the Defense Production Act, that civilian agencies have those roles of prioritizing and allocating resources. It is so that we don't disrupt.

But in this case we had, I think, a very effective load-out scenario. We moved more cargo during that 6-month period than we did during the entire Korean War. It worked very well, very efficiently. The Government agencies that were involved in the Port Readiness Network worked very well together. We established communications. We did, during that engagement, establish secure communications with all the ports. We had a credentialling system that we stood up almost overnight. It worked very well, and I think we learned a lot of good lessons from that.

Mr. PUTNAM. Let me come back to that. General, you mentioned that your committees, your Readiness Committees, have essentially shifted from being Readiness Committees to being Security Committees. Could you elaborate on the consequences of that shift?

General PRIVRATSKY. I didn't mean to imply that we have shifted, but we are shifting. On September 11th the risks to our homeland were different than they are today, and when Port Readiness Committees met routinely, quarterly in most cases, at the 13 commercial strategic ports, they met to discuss the readiness of the port to deploy the forces. Less time was spent then discussing security implications because we were perceiving the environment differently than we do today.

Now, when those Port Readiness Committees meet there is an open discussion of intelligence information. All those committees

have met at those 13 commercial ports since February. The ones in California have met just this month. There is an open dialog sharing of intelligence information.

Our ability to provide information to those committees is much better today than it was in September. As I mentioned in my written and oral testimony, we have a more robust intelligence capability in my command, and our links to other commands are better. That information throughout the Military Traffic Management Command is disseminated down to the level where they enter that Port Readiness Committee.

Mr. PUTNAM. Thank you. My time has expired.

The gentleman from Massachusetts, Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman.

Thank you, gentlemen, for your testimony.

Admiral Pluta, before September 11th or immediately following September 11th the Coast Guard was very involved in protective activities, am I right?

Admiral PLUTA. Yes, sir.

Mr. TIERNEY. When you undertook those activities, did you do so under some existing memorandum of agreement with various other agencies, or just a plan that the Coast Guard had designed on its own to spring into action?

Admiral PLUTA. I don't think I could point to a memorandum of understanding that caused us to do what we did on September 11th, we just did what we always do—we respond. We are a response organization. We saw a need and we didn't know where the next threat was coming from, so we put everything we had to work guarding the ports of the United States of America, sir.

Mr. TIERNEY. And since that day have you changed that posture at all? Are you still performing under that sort of independent mandate, or have you since then worked out memorandum of agreement or other arrangements with other people to divide up the responsibilities and address them?

Admiral PLUTA. There has been a lot more networking, sir, with regard to everything that we do in the ports, obviously. We have gone back to the traditional missions with the assets that we pulled out of service to go and defend the ports, and so that we could get back to the important drug interdiction, migrant interdiction, safety of life at sea, fisheries enforcement, those missions. But in the ports, themselves, we recognize that we couldn't do this job alone and we shouldn't do this job alone. It shouldn't be just borne by the Federal Government. It should be borne by all the agencies, as well as State and local, as well as the private sector. So we've outreached a lot, we've had a lot of public meetings, we've sent out guidance. We are working internationally to get a global solution to our problems. And, yes, sir, we are a networking organization because of how small we are, and we exercise that to the max.

Mr. TIERNEY. Has there been any conversation with the Coast Guard and the Department of Defense with respect to plans announced by the Department of Defense to do a Northern American Command?

Admiral PLUTA. Yes, sir. We have been in at the ground floor on the development of NORTHCOM all along the way, and we intend to ensure that Coast Guard is strongly represented as a member

of that staff, with your approval, with a flag officer as well as a robust staff to support that flag officer and the northern commander.

Mr. TIERNEY. What do you know so far about the plans of how the Coast Guard's responsibilities and the Navy's responsibilities will play off one another as that develops?

Admiral PLUTA. If anything, the September 11th event has caused our relationship to even strengthen. We had a NAVGUARD Board to coordinate our issues before, and resources largely flowed from the Coast Guard to the Navy. But, due to the fact that we are the lead Federal agency for maritime security, the Navy has chopped vessels for our use to protect the ports of the United States and have worked ever more closely with us on sharing intelligence, doing analysis, and our day-to-day operational readiness.

Mr. TIERNEY. And as far as you can tell, is that the direction that this NORTHCOM is heading in—that it will continue to be a cooperative relationship and that the Navy will share resources——

Admiral PLUTA. Yes, sir.

Mr. TIERNEY [continuing]. As opposed to having any sort of disturbance as to who is going to control what?

Admiral PLUTA. Yes, sir. It has been a very cooperative effort and I think the NORTHCOM is going to be focused on the maritime defense as opposed to maritime security, the preventive part of it. But the Coast Guard is integral to both of those issues, so we have been welcomed. One of my capstone classmates is putting that together for the Department of Defense. Very close relationship, sir.

Mr. TIERNEY. Thank you. I yield back the balance of my time.

Mr. PUTNAM. Thank you, Mr. Tierney.

We're going to finish out the first round with the other gentleman from Massachusetts, Mr. Lynch, and then have a second round for those who have additional questions.

Mr. LYNCH. Thank you, Mr. Chairman.

Admiral, Commander, Captain, thank you very much for your courtesy in appearing before this committee and informing us.

I want to say that I represent the Port of Boston, especially a significant portion of the maritime port. I share that honor with Congressman Capuano and also Mr. Tierney.

I just wonder if, in speaking of these 14 "strategic ports" through which we move military personnel and material, are there any lessons that can be learned for the other? I'm hoping, by the way, that the Port of Boston is on this larger list of 55 ports. I don't know. I don't have that classified list yet, but I will have it soon. Are there lessons that we can learn, structurally or in terms of preparation, to address the concerns that you see in these "strategic ports" that would be useful in the larger grouping of 55 ports? Anyone?

Admiral PLUTA. Thank you, Mr. Lynch. I think the rest of the ports can learn very from those ports. Having been a chairman of a Port Readiness Committee and having had that history since the 1980's, where the Port Readiness Network matured, it helped us prosecute the Gulf War in all our ports because the MTMC commander, the Coast Guard Captain of the Port, the State Port of North Carolina in that case, we all knew each other, our people

knew each other, we knew each other's facilities, and it was natural for us to flow into an accelerated mode.

In the other ports there were no Port Readiness Committees, and so I think part of the pending legislation that the conferees are working on and maritime security is to have a legal requirement that there be Port Security Committees in those other ports to perform largely the same function with also some additional members, like from the intelligence community and the Federal and State and local law enforcement community—FBI, State police, those kind of folks—to make sure that threat information is fresh and new.

So the lessons learned for me, sir, are that the Port Readiness Committee concept works and we ought to export that success to the other ports of the United States.

Mr. LYNCH. The other question I had is regarding containerized cargo. I know that a very small percentage of that is being inspected right now, and I know you spoke earlier of the efforts to move our borders out, so to speak, so that there is some type of screening process that might occur if we have some indication that there might be questionable persons or cargo on a particular ship. But are there any, I guess, systematized processes that you see being implemented in the near term that might address the problem that we have, for example, in the Port of Boston where we have, you know, shipping lines from China and from the Middle East and from Europe—well, the Mediterranean, let's say—coming on a weekly basis into the port of Boston?

Captain SCHUBERT. I would like to address this first, and if you want to add, Admiral—first of all, I wanted to mention it earlier with regards to the container movement of container cargo, that in this area there has been very good cooperation amongst all the Federal agencies to address this issue. In fact, as we speak right now there is what we refer to as the "inter-agency container working group" working on it up at the Merchant Marine Academy up at King's Point from Monday to Wednesday to try to consolidate and come up with some additional action items to address this issue.

Our main concern I think is, as you say, pushing the borders out is that we want to know—we want to have some form of pre-inspection of cargo and screening cargo before it is actually loaded on a ship that's coming to the United States. But, again, there is some specific recommendations from this container working group. The first report was last February, in that timeframe. Some of those initiatives have been implemented, and it is an example of very close cooperation amongst all the Federal agencies.

Admiral PLUTA. Mr. Lynch, just to inform the committee, there are several pilot projects going on under the umbrella of Operation Safe Commerce. One that has already been completed followed a containerized shipment of lights from a manufacturer in Slovakia through Germany to Canada and then down to New England. We are learning our lessons there.

There are other pilot projects on the west coast. I know the Port of Seattle is forming some bilateral partnerships and pilot projects with Singapore and with China, several ports in China, and so we

are learning how to do that, how to maintain the integrity of those pieces of cargo.

Also, a lot of this has to do with information sharing—the required proper manifesting of information and getting it to the people who need it in a timely fashion, protecting the commercial interests but allowing the Government agencies to draw from it. So we put out a notice of proposed rulemaking on our 96-hour advanced notice of arrival requirements to require that electronic cargo manifest information be forwarded directly to U.S. Customs at least 96 hours before a vessel arrives here.

So the coordination, the providing of that sort of an electronic data base and information sharing capability I think is key to our getting this, and supporting through R&D or Federal funds the kind of pilot projects where we can learn to do this properly.

Thank you, sir.

Mr. LYNCH. Thank you. Admiral, just on that last point—and this is my last question—what type of penalty befalls a company—let's just say on your very point where the bill of lading has to say, you know, exactly what is in the container that is coming into the port. Let's just say that is not—that the bill of lading is not correct, that a shipper is actually putting things in a container that he has not declared on the invoice, and that there is potentially a breach of security. What happens to that shipper who is in violation?

Admiral PLUTA. Mr. Lynch, sir, we're working with the Department of Justice on how to best structure the legal framework for penalties, but at the very minimum if somebody fails to comply with the 96-hour advanced notice of arrival requirement they won't be permitted in port, and that's going to interrupt their supply chain, and that's going to slow down their business, and they're not going to put themselves in that position if they are a competent operator. So that's one measure, and, as I said, the Department of Justice is helping us to deal with that.

If I might, may I transfer the floor to——

Mr. LYNCH. Sure.

Captain SCHUBERT. If we're talking about an issue of cargo description as manifested, it would refer to as a "misdescription of cargo," and that really falls within the realm of the Federal Maritime Commission.

Now, if we're talking about misdeclaring cargo at customers, then I'm sure there are penalties there, but the—for a misdescription of cargo, the Federal Maritime Commission does have pretty steep penalties for that.

Mr. LYNCH. It just seems to me that we are going to need the cooperation of foreign shippers to police their own cargo or their own containers before they come into this country in an effort to move the borders out.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Lynch.

Let me just ask a quick question to followup from Mr. Lynch before we yield to the chairman.

In 1998, according to testimony that this subcommittee received last week, 1998 a private weapons collector imported not one but two scud missiles from Czechoslovakia into the Port of Long Beach. What was the penalty to the shipper for mis-identifying, or how did

we correctly identify that scud missiles were coming in and no one caught it?

Admiral PLUTA. I can't answer your question, Mr. Chairman. I was unaware of that event. It's a Customs declaration kind of an issue. I can't speak for them. I'm sorry, sir, but I can't answer.

Mr. PUTNAM. Thank you.

Mr. Chairman, you are recognized.

Mr. SHAYS. Thank you, Mr. Chairman.

I almost would be overwhelmed if I had to figure out how to protect our ports, in part because almost every military part, it strikes me, is a domestic port—I mean, has a non-military function, as well. Is that fairly accurate, Captain?

Captain SCHUBERT. Yes. I'd say that, from a percentage basis of cargo that's moving through our ports on a regular basis, it's a very small percentage. A very small percentage of our cargo would be DOD cargos, if that's what you're asking.

Mr. SHAYS. When I was asking earlier about the whole issue of vulnerability and threat assessment, I'm unclear as to what agency is responsible for conducting seaport-specific terrorism vulnerability and threat assessment.

Captain SCHUBERT. I would view that—as I mentioned earlier, the Coast Guard has gone out to develop a very detailed, comprehensive port—we don't call it port vulnerability assessments—port security assessment on a way to do that on the 55 ports, and I believe Admiral Pluta could address that, but I believe the Coast Guard, as our primary agency for homeland security, is responsible for that.

Admiral PLUTA. Mr. Chairman, if I might add?

Mr. SHAYS. Yes. Sure.

Admiral PLUTA. Thank you, Mr. Chairman. As I mentioned earlier, we have sought funds and received some to conduct vulnerability of port security assessments here at the—at first the most important ports in the United States, and eventually all of them. This would be a comprehensive assessment by a contractor with Coast Guard oversight to look at all aspects of vulnerability of the entire port, not just a single facility.

I think, to contrast with what General Privratsky was talking about, he is mainly concerned, I believe, with the facility, itself, under MTMC and worrying about it from both the shore side and the water side. Our concern is the entire port. One facility may be very well protected and the one right next door not well protected. We want to uncover those kind of vulnerabilities and look at such things as where do they get their power from, how well is their information protected, and then how is access control provided, lighting, fencing, the whole nine yards.

Mr. SHAYS. And I make an assumption that you have not had the resources to do it so we do not at this time really have an assessment of vulnerability and threat. I mean, we are doing it but we don't have it.

Admiral PLUTA. Yes, sir. We have five completed. We hope to do eight at least this year with the funds available to us.

Mr. SHAYS. And how many are we talking about?

Admiral PLUTA. I'm sorry, sir?

Mr. SHAYS. How many would we be talking about totally?

Admiral PLUTA. Fifty-five, sir.

Mr. SHAYS. And so, General, would you kind of, based on what the admiral told me, put it in context with what you were telling me about?

General PRIVRATSKY. The fifty-five, seventeen of those ports are strategic ports, and of those thirteen are commercial, and of those thirteen there have been risk assessments conducted on four of the commercial ports. Of the DOD facilities, there have been extensive risk assessments done on two, those at Sunny Point, North Carolina, and Concord, California.

Mr. SHAYS. And are those ports—sorry for my ignorance—are those ports exclusive military, or are they ports that folks sail out of for pleasure and commercial ships come in?

General PRIVRATSKY. Our port at Sunny Point, North Carolina, is a DOD installation. It is our primary port for shipping ammunition. We do have——

Mr. SHAYS. These are weapons ports. I'm sorry, but what I'm asking is—the ports are fairly large, so do you have a part of a major harbor or——

General PRIVRATSKY. These are exclusive use Department of Defense facilities. At Sunny Point I do have the capability and the approval authority to move commercial shipments through there, and I have executed that a half dozen times in the past year-and-a-half through an extensive coordination process.

Mr. SHAYS. Let me just conclude by asking each of you to do a proper threat—to do the things that were mentioned by GAO, the comprehensive assessment of threat, vulnerability, and critical port infrastructure and functions, to do the proper overseeing, coordination, executing force protection, what type of dollars are we talking about?

Admiral PLUTA. Mr. Chairman, the assessments—average cost of a comprehensive assessment of an entire port area like I have been talking about is about $500,000, a half million dollars apiece to do that.

Mr. SHAYS. And if you had all the money necessary, would you have the personnel to do it, or is there a time issue, as well? I mean, in other words, is there a limit to how quickly we can do this?

Admiral PLUTA. Mr. Chairman, I think there is—we could do it quicker than we have planned right now. We are using a contractor, and we are going to—the Coast Guard role and our other agencies that are helping us do oversight are going to just be overseeing the contractor's work. So it is a matter of how many people the contractor can get geared up to do the job. They have been working on first a model port assessment template that we can apply to every port, not that one size fits all, but we need to look at the same elements as we look at every port. So that work is nearly complete, and then they will be ready to roll it out and try it out on ports.

We have learned what we've learned today through working with DTRA on threat reduction to defense ports, but it is—I think it is more resource constrained than time constrained, Mr. Chairman.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much.

Mr. PUTNAM. Mr. Chairman, thank you.

At this time we recognize the distinguished chairman emeritus of the International Relations Committee, Mr. Gilman.

Mr. GILMAN. Thank you, Mr. Chairman.

I address this to the entire panel. I regret I had to go to another meeting and was detained from coming back on time. What is the role of the Merchant Marine in port security or security in high seas? Can I address that to the whole panel?

Captain SCHUBERT. Well, first of all, in my opinion, the safest way to move cargo is under—is on a U.S.-flagged vessel with U.S.-owned and U.S.-crewed crew on board the ship. That is the basis for the Cargo Preference Act of 1904 which mandates that all military cargo move on U.S.-flagged ships.

But the bit for security, it is—I certainly feel better, you know—I gave some testimony a couple of weeks ago about some of the issues around what we call "open registries, flag inconvenience." So we are quite concerned that some of these ships that are coming in and out of our ports, that we need to increase the knowledge and standardized way of credentialling worldwide so we know who is on those ships.

Outside of that, we have the IMO efforts that the Coast Guard is engaged in, which I believe will designate a security officer aboard our ships.

Did you want to add to that, Admiral?

Admiral PLUTA. If I may, Mr. Chairman Emeritus, thank you, sir. What the administrator said is true. We are depending upon the mariner to be our eyes and ears, as well as making sure that the vessel security plans that we will require both domestically and internationally for all flagged vessels, there be a vessel security officer on board designated to make sure that the security measures are implemented on that ship, and that could be things like making sure you know all of the crew members and passengers on board and whether or not they are clean, making sure that any of the cargo—all the cargo on board has been properly vetted, and those sorts of things. We also will require a company security officer to oversee their whole fleet of ships, likely to be a former Merchant Mariner.

Mr. GILMAN. Admiral Pluta, is there some special training for these security officers on each ship?

Admiral PLUTA. Yes, sir, there will be a list of required competencies that they have to have and required training that they have to have, and then they have to train the rest of the crew in what their responsibilities will be.

Mr. GILMAN. Who will be doing that training initially?

Admiral PLUTA. You want to answer that?

Captain SCHUBERT. We're still waiting for the pending legislation to port security to pass, and it will address that to some degree, but from the viewpoint of the Department, we believe that we have resources out there like the U.S. Merchant Marine Academy at King's Point and Global Maritime Transportation School at King's Point that can be used for that.

Mr. GILMAN. But they're not using them at the present time; is that correct?

Captain SCHUBERT. I could say not only the Merchant Marine Academy, but the State schools are implementing security courses at their schools as we speak, but, as I mentioned in my opening statement, the Global Maritime Transportation School at King's Point is currently training—actually, in August will be training from the State of Florida law enforcement officers from the State of Florida, and this will be, I think, the first real class dedicated exclusively to do that.

Mr. GILMAN. So right now there is no overall training in place; is that right?

Captain SCHUBERT. It's not—correct, sir. It's not in place yet because we were waiting for the final legislation to come out of conference to see how it will define those responsibilities.

Mr. GILMAN. I hope you are going to be able to expedite that. How do we currently monitor private boat owners from international ports like yachts, fishing vessels? How do we monitor all of that?

Admiral PLUTA. Mr. Chairman Emeritus, I don't think that we monitor. We monitor the vessels that do come into the United States, but, as far as the private vessels, I don't think there is—they're below the cutoff for our 96-hour advanced notice of arrival requirements. We hope to get all vessels under that same requirement so that we can see all foreign yachts and foreign fishing vessels and foreign other vessels coming into the United States, but currently we have no requirement for that, sir.

Mr. GILMAN. So right now, Admiral, they are under the radar screen, right? They're not up on the screen?

Admiral PLUTA. Yes, sir.

Mr. GILMAN. Thank you very much.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Chairman.

We appreciate the distinguished panel's comments. There may be additional comments submitted for you to answer for the record. At this time we will excuse the first panel and seat the second panel.

The subcommittee is pleased to welcome Mr. Raymond Decker, the director of Defense Capabilities and Management Team with the U.S. General Accounting Office, and Mr. Kenneth Goulden, Vice President of Maersk Sealand. Welcome to the subcommittee, gentlemen.

As you know, this is a subcommittee that does swear in witnesses, so I would ask that you please stand and raise your right hand.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that the witnesses responded in the affirmative.

It is a pleasure to have you with us, and we will begin with Mr. Decker. You are recognized.

STATEMENTS OF RAYMOND DECKER, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT TEAM, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JOE KIRSCHBAUM, SENIOR ANALYST; AND KENNETH GOULDEN, VICE PRESIDENT, MAERSK SEALAND

Mr. DECKER. Thank you very much, Mr. Putnam, Chairman Shays, distinguished members of the subcommittee. I am pleased to be here today to participate in a hearing on homeland security, securing strategic ports with an emphasis on the security coordination measures through our military movements through these vital portals.

As requested, my testimony will focus on the security environment at domestic strategic seaports used by the Department of Defense for military deployments and the Department's process for securing these military deployments through those ports. My comments are based on preliminary results of the work we are currently conducting on this issue for the subcommittee. We plan to provide the subcommittee with a report this fall.

I have asked my senior analyst in charge responsible for this area, Mr. Joe Kirschbaum, to join me at the witness table.

The October 12, 2000, attack on the U.S. destroyer "U.S.S. Cole" in the Port of Aden illustrated the danger of non-traditional threats to U.S. ships in seaports. The September 11th attacks heightened the need for a significant change in conventional anti-terrorism thinking. The new security environment assumes that all U.S. military assets here and abroad are vulnerable to attack and a domestic physical infrastructure such as our commercial seaports is recognized as highly vulnerable to potential terrorist attack. These seaports are vital to our national security, and during a major conflict 95 percent of the Department of Defense's equipment and material needed for overseas military operations would pass through them.

Uncertainties regarding the seaport security environment exist for several reasons. First, comprehensive assessments of threat, vulnerability, and critical port infrastructure and functions which we would call "criticality" have not been completed. These assessments underpin the risk management approach that I have previously described in past hearings before this subcommittee and the Senate Committee on Governmental Affairs.

As you are aware, risk management is a balanced, systematic, and analytical approach to determine the likelihood that a threat could adversely affect individuals, physical assets, or functions, and then identify actions to reduce the risk, mitigate the severity of the consequence of the event, and reasonably manage uncertainty.

Second, no effective process exists to receive, analyze, evaluate, and disseminate the spectrum of threat information at seaports. Most threat information at the ports is received informally through personal contacts with law enforcement individuals. No formal mechanism exists to ensure that all threats are factored into the risk-based decisionmaking process with actionable information transmitted in a timely manner to all relevant organizations.

Recent efforts by the Coast Guard and other agencies at the ports are attempting to address many of these weaknesses, and you heard many of the witnesses in the previous panel discuss this.

The Coast Guard has initiated vulnerability assessments of the port's infrastructure and is deploying additional teams dedicated to seaport authority functions. The first Marine safety and security team was deployed 3 weeks ago to Seattle and will provide SWAT-team-like support to investigate suspicious vessels before they enter U.S. ports.

In 1999, the Coast Guard discussed in a strategic plan the concept of maritime domain awareness, which links information fusion, risk management principles, and decisionmaking process. With the support of the National Security Council, this concept is being validated at the Coast Guard's Intelligence Coordination Center in Suitland through real-world application.

On the congressional front, proposed legislation, Senate Resolution 1214, the Port and Maritime Security Act of 2001, should assist those officials and organizations responsible for the safe and secure operation of our seaports to better focus resources and actions against future threats. Several key provisions of the legislation include: the establishment of a national level and port and local port security bodies to plan and oversee security measures, the conduct of port vulnerability assessments, and background checks for port workers and development of access controls to sensitive areas. There is much more in that resolution that will be very beneficial.

The implementation of these provisions and others will help create an effective framework to better understand the threat environment and the importance of the continuous assessment of threat to support daily operations, as well as short-and long-term planning. We believe the current enhanced security-related activities discussed earlier, coupled with the measures of S.R. 1214, should continue to improve the security posture of our seaports.

Now I would like to comment on Department of Defense's force protection process for deployments through domestic seaports. During the conduct of our work, we identified two significant weaknesses in the process. First, there is no Department of Defense focal point tasked to provide overall oversight, coordination, and execution of domestic force protection measures from fort-to-port military movements. Since a military movement of equipment or material normally involves the parent military unit, the Military Transportation Management Command, Port Readiness Committee, Military Sealift Command, and with each of these elements responsible for a different portion of the journey, there are varying degrees of force protection planning, execution, and risk management application.

Complicating this issue further is the fact that non-Government parties may be contracted to provide transport by road and rail. As a result, potential force protection gaps and weaknesses requiring attention and action outside the purview or awareness of any one element may exist.

In contrast, once a military shipment reaches its overseas debarkation point, a military element at the Unified Command level is responsible for the overall force protection planning and execution for the safe off-load and transport to its final destination. This capability provides oversight of all phases of the movement, especially when non-U.S. entities are involved.

Second, during the movement of military equipment or material by ship, the Department sometimes relinquishes control of these items to non-Department-of-Defense entities to include foreign-flagged ships crewed by non-U.S. citizens. Although this practice is consistent with current Department policies and procedures, it limits the Department's ability to provide security oversight while the equipment is in transit and potentially increases the risk involving these vital cargos.

In summary, Mr. Chairman, the events of September 11th heightened the vulnerability of the U.S. homeland to non-traditional attack, and the resulting new environment warrants that more attention be focused on vital military deployments through strategic commercial seaports.

A risk management approach will wisely guide both military and civilian leaders and managers as they make important decisions affecting planning and actions to better prepare against potential attacks and mitigate the consequences of adverse events. However, the current uncertainties in the security environment at our domestic ports and weaknesses in the Department of Defense's force protection approach increase the potential risk to military deployments that could adversely affect U.S. overseas operations.

Mr. Chairman, this concludes my statement. We would be pleased to respond to any questions you, the committee, may have.

Mr. SHAYS [resuming Chair]. Thank you, Mr. Decker. I appreciate all the work you do before this committee.

[The prepared statement of Mr. Decker follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m., EST
Tuesday, July 23, 2002

COMBATING TERRORISM

Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports

Statement of Raymond J. Decker
Director, Defense Capabilities and Management

GAO-02-955TNI

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in this hearing on security for military mobilizations through strategic[1] seaports. The October 12, 2000, attack against the Navy destroyer U.S.S. *Cole* in Aden illustrated the danger of unconventional threats to U.S. ships in seaports. The September 11 attacks heightened the need for a significant change in conventional antiterrorist thinking. The new security environment assumes that all U.S. forces, be they abroad or at home, are vulnerable to attack, and that even those infrastructures we traditionally considered of little interest to terrorists, such as seaports in the continental United States, are now commonly recognized as highly vulnerable to potential terrorist attack. These seaports are vital to national security. During a major war, the Department of Defense (DOD) would transport more than 95 percent of all equipment and supplies needed for military operations by sea.

Military commanders are required to protect personnel, equipment, and assets. To achieve this, commanders are required to apply a risk management approach. "Risk management" is a systematic, analytical process to determine the likelihood that a threat will harm physical assets or individuals and to identify actions to reduce risk and mitigate the consequences of an attack. The principles of risk management acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can serve to significantly reduce risk.

As requested, my testimony focuses on (1) the security environment at domestic strategic seaports used by DOD for military deployments and (2) DOD's process for securing military deployments through those ports. My comments are based on preliminary results of work we are currently conducting for the Subcommittee on force protection for deployments through commercial seaports in the United States. We plan to provide the Subcommittee with a report in October that will include recommendations, as appropriate. To perform our analysis, we visited 6 of the 14 designated strategic commercial seaports in the United States, 2 military-owned ammunition ports, and 3 military installations from which unit equipment was deployed overseas in 2001. At the seaports and military installations, we reviewed planning documents, interviewed a

[1] Strategic seaports are those that would be needed by the Department of Defense in case of a major war.

broad range of officials from several executive departments, and observed security measures.

Summary

Uncertainties regarding the seaport security environment exist because comprehensive assessments of threat, vulnerability, and critical port infrastructure and functions have not been completed, and there is no effective mechanism to coordinate and disseminate threat information at the seaports. These conditions compound the already difficult task of protecting deploying forces and increases the risk that threats—both traditional and nontraditional[2] ones—may not be recognized or that threat information may not be communicated in a timely manner to all relevant organizations. Recent efforts by the Coast Guard and other agencies at the ports have begun to address many of these weaknesses. The Coast Guard has initiated assessments of port vulnerability and infrastructure and is deploying additional teams dedicated to seaport security functions. Further, legislation currently before the Congress proposes steps that may assist these efforts and provides for additional measures that could improve the coordination and dissemination of threat information.

We identified two significant weaknesses associated with DOD's force protection process for deployments through domestic seaports. First, DOD lacks a central authority responsible for overseeing, coordinating, and executing force protection measures while military forces deploy from domestic installations through U.S. seaports. As a result, potential force protection gaps and weaknesses requiring attention and action might be overlooked. DOD has such an authority for the overseas portions of deployments and is therefore better able to identify and mitigate force protection gaps there. Second, during some stages of a deployment DOD relinquishes control over its military equipment to non-DOD entities, including foreign-owned ships crewed by non-U.S. citizens. Although these practices are consistent with current DOD policies and procedures, they limit DOD's ability to oversee security measures. As a result, equipment could fall into the hands of individuals or groups whose interests run counter to those of the United States.

Background

DOD defines force protection as "security programs designed to protect service members, civilian employees, family members, facilities,

[2] Nontraditional threats can include natural or man-made disasters, such as hurricanes, industrial accidents, and cyber attacks.

information, and equipment in all locations and situations, accomplished through the planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and security programs."[3] Our review concentrated mostly on the physical security and related aspects of force protection that include measures to protect personnel and property and encompass consequence management, intelligence, and critical infrastructure protection.

We have identified a risk management approach used by DOD to defend against terrorism that also has relevance for the organizations responsible for security at commercial seaports. This approach can provide those organizations with a process to enhance levels of preparedness to respond to terrorist attacks or other national emergencies, whether man-made or unintentional in nature. The approach is based on assessing threat, vulnerability, and the importance of critical infrastructure and functions (criticality).

Threat assessments identify and evaluate potential threats on the basis of factors such as capabilities, intentions, and past activities. These assessments represent a systematic approach to identifying potential threats before they materialize. However, even if updated often, threat assessments might not adequately capture some emerging threats. The risk management approach therefore uses vulnerability and criticality assessments as additional input to the decision-making process.

Vulnerability assessments identify weaknesses that may be exploited by identified threats and suggest options that address those weaknesses. For example, a vulnerability assessment might reveal weaknesses in a seaport's security systems, police force, computer networks, or unprotected key infrastructure such as water supplies, bridges, and tunnels. In general, teams of experts skilled in areas such as structural engineering, physical security, and other disciplines conduct these assessments.

Criticality assessments evaluate and prioritize important assets and functions in terms of factors such as mission and significance as a target. For example, certain power plants, bridges, computer networks, or population centers might be identified as important to the operation of a

[3] DOD Instruction 2000.16, *DOD Antiterrorism Standards*, June 14, 2001.

seaport or the local public health and safety. Criticality assessments provide a basis for identifying which assets and structures are relatively more important to protect from attack. In so doing, the assessments help determine operational requirements and provide information on where to prioritize and target resources while reducing the potential to target resources on lower priority assets.

In the event of a major military mobilization and overseas deployment, such as Operation Desert Shield, a large percentage of U.S. forces (equipment and other materiel) would be sent by sea through a number of commercial seaports in the United States to their respective areas of operations. The military also uses commercial seaports for deployments such as the operations in the Balkans. The Departments of Defense and of Transportation have identified 14 seaports as "strategic," meaning that they are necessary for use by the military in the event of a major war. DOD has also identified two other commercial ports and three military-controlled ammunition ports as important for a mobilization surge.

Because the security activities that DOD may conduct outside its installations are limited, it must work closely with a broad range of federal, state, and local agencies to ensure that adequate force protection measures exist and are executed during deployments through strategic seaports. Force protection responsibilities for DOD deployments through commercial seaports are divided among a number of DOD organizations including the United States Transportation Command and its components (particularly the Military Traffic Management Command and Military Sealift Command), the U.S. Army Forces Command, and the individual deploying units.

A National Port Readiness Network provides a common coordination structure for DOD, the Coast Guard, and other federal, state, and local agencies at the port level. The network is comprised of Port Readiness Committees at each strategic port to provide the principal interface between DOD and other officials at the ports.

The issue of security at the nation's seaports has been the subject of a recent study, as has the broader issue of homeland security. In fall 2000, the Interagency Commission on Crime and Security in U.S. Seaports

reported that security at seaports needed to be improved in a number of areas, including

- coordination and cooperation among agencies;
- establishing guidelines for commercial facilities handling military cargo; and
- assessments of threats, vulnerabilities, and critical infrastructure at ports.

In February 2001, the Commission on National Security/21st Century (commonly referred to as the Hart-Rudman Commission) reported that threats, such as international terrorism, would place the U.S. homeland in great danger and that direct attacks on the United States were likely in the next 25 years. In addition to recommending national action, the Hart-Rudman Commission urged DOD to pay closer attention to operations in the United States.

Current Risk Management Approach Creates Uncertainties about the Security Environment at Strategic Seaports

The security environment at strategic seaports is uncertain because comprehensive assessments of threat, vulnerability, and critical port infrastructure and functions have not been completed, and therefore, agencies at seaports lack the information necessary to effectively manage risk. Recent efforts by the Coast Guard and other agencies at the ports have begun to address several important security issues, and maritime security legislation before the Congress may assist these efforts. Further, the proposed legislation may provide a framework for seaport organizations to improve the coordination and dissemination of threat information.

Weaknesses Exist in the Process to Assess Risk at Seaports

There is a wide range of vulnerabilities at seaports, including critical infrastructure such as bridges and refineries, shipping containers with unknown contents, and the enormous volume of foreign and domestic shipping traffic. Many of the organizations responsible for seaport security do not have the resources necessary to mitigate all vulnerabilities. To determine how best to address security at seaports, it is vital for responsible agencies involved to follow a risk management approach that includes assessments of threat, vulnerability, and critical infrastructure and functions. The results of these assessments should then be used to develop comprehensive security plans.

The organizations responsible for security at strategic seaports have increased emphasis on security planning. However, in these planning efforts, the organizations we visited applied the elements of risk

management differently. At only one of six ports we visited were the results of threat, vulnerability, and criticality assessments integrated into a seaport security plan that included all relevant agencies. Specific weaknesses in the risk management approach used at ports we studied include the following:

- Individual organizations at the seaports we visited conducted separate vulnerability assessments that were not coordinated with those of other agencies and were not based on standardized approaches. The Coast Guard has taken the lead in developing a standard methodology for comprehensive port-wide vulnerability assessments that it plans to complete at 50 major ports, including all designated strategic seaports.
- Assessments of the criticality of seaport infrastructure were not done at all the ports we visited prior to September 11. The Coast Guard has since addressed this shortcoming by conducting assessments of high-risk infrastructure at all major ports. It coordinated the assessments with commercial facilities at the ports.
- In some cases, threat assessment information received by affected agencies is based on higher-level regional assessments that do not focus on the local port facility. These regional assessments, while helpful in providing a broader view of the security environment, do not provide site-specific local threat information to the port.
- Agencies involved with seaport security have different concepts of standards for threat assessments and the degree to which threat information should be shared and disseminated. Some agencies have not traditionally shared threat information as widely as may be necessary for comprehensive security measures at seaports.

In addition to these specific weaknesses, we found that there is no single entity at the seaports we visited to analyze, coordinate, and disseminate information on the broad range of threats at each port on a routine basis. Most threat information at the ports was coordinated on an informal basis, such as through personal contacts between law enforcement individuals and those at other agencies. The lack of such a mechanism compounds the already difficult task of protecting deploying military forces and increases the risk that threats—both traditional and nontraditional ones—may not be recognized or that threat information may not be communicated in a timely manner to all relevant organizations. Currently, interagency bodies that may exist at or near these ports, such as Port Readiness Committees, Joint Terrorism Task Forces, or the newly formed Antiterrorism Task Forces, do not routinely focus specifically on coordinating threat information focused solely on the ports, and they were not designed to do so.

The Interagency Commission on Crime and Security in U.S. Seaports noted in 2000 the importance of interagency threat coordination. Officials at seaports need a means to analyze, coordinate, and disseminate information on the broad range of threats they face. This includes information on ships, crews, and cargo, along with criminal, terrorist, and other threats with foreign and domestic origins. Although the commission did not recommend centralizing threat information distribution into a single agency or regulating dissemination procedures at seaports, it did recommend improvements in integrating threat information systems and improved coordination mechanisms for law enforcement agencies at the seaport level.

In prior work, we reported that DOD uses Threat Working Groups at its installations as a forum to involve installation force protection personnel with local, state, and federal law enforcement officials to identify potential threats to the installation and to improve communication between these organizations.[4] These coordination mechanisms can help coordinate as much information as possible on a broad range of potential threats. Given the limited information on threats posed by less structured terrorist groups or individuals, such a mechanism assists the installation commander and local authorities in gaining a more complete picture of internal and external threats on a more continuous basis over and above an annual threat assessment.

Recent Efforts and Proposed Legislation May Assist Port Security Improvements

Since the September 11 attacks, the Coast Guard and other agencies at ports have made efforts to improve risk management and security measures. The Coast Guard, traditionally a multimission organization, has refocused most of its efforts on waterside seaport security. In so doing, it has diverted resources from other missions such as drug interdiction. Examples of additional recent efforts by the Coast Guard and other agencies include

- formation of Coast Guard Marine Safety and Security Teams based at selected ports to assist in providing port security personnel and equipment;
- Coast Guard escorts or boarding of high-risk ships, including cruise ships in ports;

[4] *Combating Terrorism: Actions Needed to Improve Antiterrorism Program Implementation and Management* (GAO-01-909, Sept. 19, 2001).

- Coast Guard escorts for naval vessels;
- establishment and enforcement of new security zones and increased harbor security patrols; and
- port authority cost estimates for improving facility security and interim security improvement measures.

Legislation on maritime security currently before the Congress (in conference)[5] may promote and enhance these seaport security efforts. Some of the major provisions include

- vulnerability assessments to be conducted at ports;
- establishment of Port Security Committees at each port, containing broad representation by relevant agencies, to plan and oversee security measures;
- development of standardized port security plans;
- background checks and access control to sensitive areas for port workers; and
- federal grants for security improvements.

On the basis of our discussions with agency officials at the ports we visited, we believe that if enacted and properly implemented, these and other provisions of maritime security legislation should assist these officials in addressing many of the weaknesses we have identified. For example, comprehensive vulnerability assessments and the proposed standardized security plans could provide a more consistent approach to identifying and mitigating security weaknesses. In providing for port security committees and interagency coordination, the legislation also provides a framework for organizations at seaports to establish a mechanism to coordinate, analyze, and disseminate threat information at the port level. There may be challenges, however, to implementing this legislation, including opposition to provisions for background checks for port workers.

[5] S. 1214 passed the Senate on December 20, 2001. The House of Representatives passed an amendment to S. 1214 on June 4, 2002.

Weaknesses in DOD Force Protection Process Increase Risks for Deployments Through Domestic Seaports

During our review, we identified two weaknesses in DOD's force protection process. First, DOD lacks a central authority responsible for overseeing, coordinating, and executing force protection measures at the domestic stages of military deployments through U.S. seaports. As a result, potential force protection gaps and weaknesses requiring attention and action might be overlooked. Second, there are instances during some stages of a deployment in which the Department relinquishes control over its military equipment to non-DOD entities. At these stages, the equipment could fall into the hands of individuals or groups whose interests run counter to those of the United States.

DOD Lacks a Central Authority to Coordinate and Execute Domestic Force Protection Measures

Deploying units traditionally focus their force protection efforts primarily on their overseas operations. Before they arrive in an overseas region, the units are required to submit force protection plans to the unified combatant commanders,[6] who are responsible for force protection of all the military units in their region. The tactics, techniques, and procedures in the units' plans must match the guidance developed by the unified commander, who coordinates and approves the individual plans. This allows the commander to ensure that a unit's plan has taken into account all current threats that could affect the mission and to accept or mitigate any security risks that arise.

The situation for the domestic stages of a deployment is different: there is no designated commander with similar centralized force protection responsibilities as those of the overseas unified combatant commander. This creates gaps during the domestic stages of a deployment in DOD's ability to coordinate individual force protection plans, identify gaps that may exist, and mitigate or accept the identified risk. The one coordination mechanism that is in place—the Port Readiness Committees I previously mentioned—are focused solely on port operations and do not coordinate all stages of a deployment from an installation through a port.

In the deployments we reviewed, we found that service guidance and DOD antiterrorism standards, particularly those that emphasize the elements of risk management (such as Army major command force protection operations orders), were not always followed in all phases of a deployment from an installation through a port. For example, the Military Traffic Management Command prepared security plans for port operations

[6] Previously called the Commanders-in-Chief.

during a deployment that were based on assessments of threats, vulnerabilities, and critical infrastructure. However, the transport of military equipment to the port by commercial carrier was not always accompanied by such detailed plans and assessments.

Military Equipment and Cargo Are Sometimes Not Under DOD Control

During deployments from domestic installations through commercial seaports, there are three phases in which DOD either relinquishes control of its equipment to non-government persons (in some cases foreign nationals) or does not have adequate information about who is handling its equipment.

- Private trucking and railroad carriers transport equipment and cargo from military installations to seaports.
- Civilian port workers handle and load equipment onto ships.
- Private shipping companies with civilian crews sometimes transport DOD equipment overseas.

The deployments we reviewed from three military installations in calendar year 2001 involved the use of road and rail contract carriers transporting equipment from a military installation to a port of embarkation, and all transports took place in accordance with DOD regulations. Contract carriers are required to provide security for the equipment they transport, including sensitive items. Although we did not review the steps taken by DOD to evaluate the contractors' security measures, the transfer of accountability to these non-government agents creates a gap in DOD's oversight of its assets between installations and ports.

Once equipment arrives at a commercial seaport, it comes under the control of military units responsible for managing the loading process at the port. However, civilian port workers, stevedores, and longshoremen—with limited screening and background checks by port authorities, or terminal operators—handle military equipment and cargo, as well as the loading and unloading of ships used to transport the equipment overseas. This was the case in all the deployments we reviewed. The stevedores or longshoremen were in the same labor pool as the one used for commercial port operations. Organizations at some of the ports we visited are now implementing or reviewing efforts to increase screening of port workers. Maritime security legislation before the Congress includes provisions for background checks and access control for port workers. These measures, if passed, may help address this issue.

DOD also relinquishes control of its equipment when the equipment is placed aboard a commercial ship for transport overseas. The Military Sealift Command sometimes contracts or charters foreign-flagged vessels to transport military equipment. The Command reviews charter vessel crew lists to determine whether any crewmembers are known security threats. The deployments we reviewed, however, used foreign-flagged vessels with non-U.S. citizen crewmembers, including some from countries with known terrorist activities, who received and transported sensitive military equipment. Although several of the ships used in the deployments we reviewed did have DOD maintenance personnel aboard, the ship manifests did not indicate that armed DOD personnel were aboard. Some of the items transported by these vessels included Bradley Fighting Vehicles, 155mm towed howitzers, and UH-60 Blackhawk helicopters, as well as smaller items such as .50 caliber machineguns; night-vision equipment; body armor; and nuclear, biological, and chemical protective gear.

When DOD relinquishes control over its equipment, it relies on non-government third parties to protect its assets. In addition, when these third parties include foreign nationals, there may be an increased risk of the equipment being tampered with, seized, or destroyed by individuals or groups whose interests run counter to those of the United States and increased chance that those weapons or equipment might be used against military or civilian targets. Additionally, placing military equipment outside DOD's control complicates the steps needed to mitigate the higher risk and could disrupt military units from performing their intended missions. DOD officials told us that the reasons for the use of commercial contract carriers include, among others, economy and efficiency over using government owned and operated vessels, and the adequacy and availability of the U.S.-flagged merchant marine.

Conclusion

The events of September 11 highlighted the vulnerability of the U.S. homeland to unconventional attack, and the resulting new security environment warrants that more attention be paid to the domestic phases of military deployments. Uncertainties in the security environment at strategic seaports and weaknesses in DOD's force protection approach result in increased risks that military operations could be disrupted, successful terrorist attacks might occur, or sophisticated military equipment might be seized by individuals or organizations whose interests run counter to those of the United States.

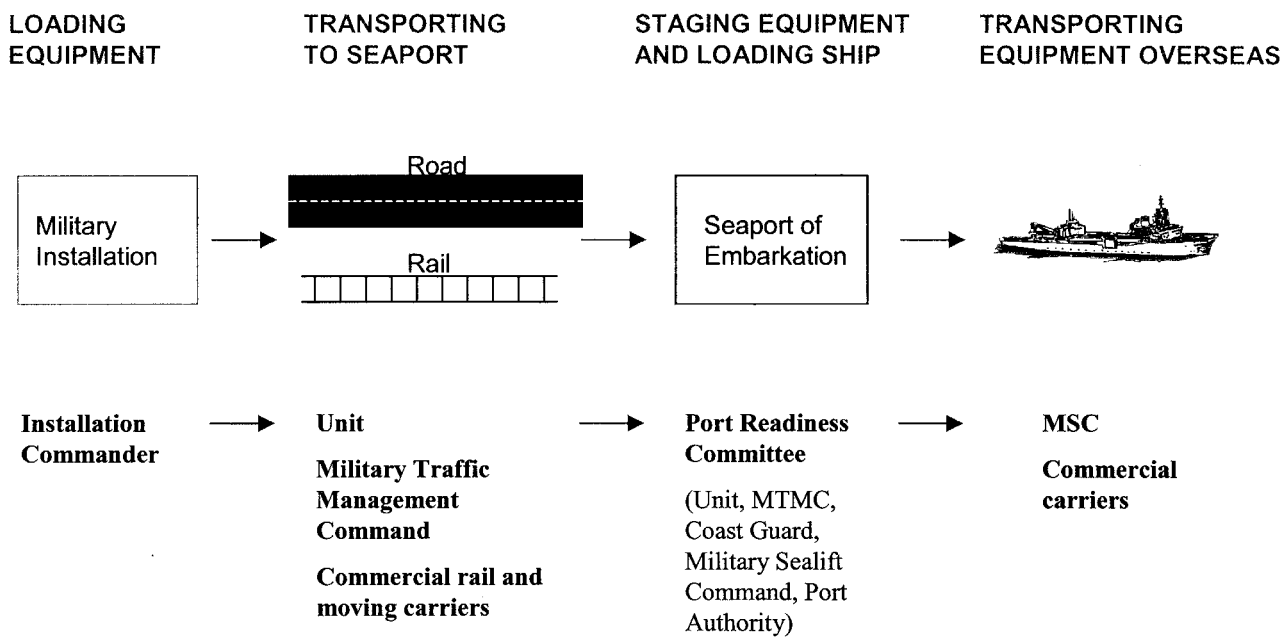
When we conclude our evaluation, we plan to provide the Subcommittee with a report in October that will include recommendations addressing (1) threat coordination at strategic seaports, (2) DOD's oversight, coordination, and execution of force protection for deployments through seaports, and (3) DOD's control over its equipment.

Mr. Chairman, this concludes my prepared statement.

Contacts and Acknowledgments

For further information about this testimony, please contact me at (202) 512-6020 or Robert L. Repasky at (202) 512-9868. Willie J. Cheely, Jr., Brian G. Hackett, Joseph W. Kirschbaum, Jean M. Orland, Stefano Petrucci, Elisabeth G. Ryan, and Tracy M. Whitaker also made contributions to this statement.

Deployment Process and Organizational Responsibilities



Mr. SHAYS. Mr. Goulden at Maersk Sealand.

Mr. GOULDEN. Mr. Chairman, members of the subcommittee, it is a pleasure for me to appear here before you today to speak about security coordination measures at strategic seaports during mobilization of military cargo. Maersk shares your commitment to ensuring that security measures are in place to protect military personnel and cargo during mobilizations.

By way of background, Maersk is one of the largest providers of global intermodal transportation services in the world. We have built and operate an integrated transportation network covering 100 countries. Our network includes more than 250 ocean-going vessels, numerous terminals on five different continents, including 12 ocean terminals here in the United States, over 800,000 shipping containers, business relationships with trucking companies and railroads around the world, and sophisticated information management systems to track each shipment from initial order to final delivery.

One of Maersk's most important customers is the U.S. Government and the Department of Defense, in particular. Two of our main business areas with the Department of Defense are, one, ship ownership and management services, and, two, global intermodal transportation services.

With respect to ship ownership management services, Maersk owns and/or operates a sizable fleet of ships exclusively for the U.S. military. The fleet includes two ammunition ships, eight large medium-speed roll-on/roll-off ships known as LMSRs, five maritime prepositioning ships, and twelve surveillance ships. These ships typically call at seaports controlled by the U.S. military.

Maersk also provides the military with global intermodal transportation services using our commercial intermodal network. Currently Maersk transports approximately 30,000 40-foot equivalent containers each year for the Department of Defense.

In addition to providing peacetime support, Maersk supports the military mobilization requirements through its participation in the maritime security program and the voluntary intermodal sealift administration known as VISA. Under these programs, Maersk has committed to provide the U.S. military with more intermodal and vessel capacity capabilities during a mobilization than any other carrier in the world. This commitment is memorialized in pre-negotiated contracts to facilitate a quick and seamless transition from peacetime to contingency operations.

Earlier, General Privratsky provided the subcommittee with testimony that focused primarily on security of military organic transportation networks. The military also relies on commercial intermodal networks and assets. The focus of my testimony is the security of commercial intermodal networks during both peacetime and military mobilizations.

Mobilizations and major deployments will be accomplished under the VISA program. One important component of the VISA program is the Joint Planning and Advisory Group known as JPAG. The JPAG provides a forum for the military and VISA carriers to exchange information, both classified and unclassified, and coordinate actions to develop concepts of operations. Through pre-negotiated contracts, the JPAG will have a number of tools at its disposal and

can incorporate these into CONOPS to protect military cargo. The security measures included in the CONOPS will be in addition to the many security measures that Maersk has in place to protect its commercial intermodal network and the cargo that moves through it.

Since September 11th, Maersk has hardened its existing security systems and procedures. Maersk also was one of the first carriers to participate in the voluntary U.S. Customs trade partnership against terrorism initiative known as C-TPAT. As part of that initiative, Maersk is conducting global security assessment and gap analysis, which should be completed within the next 30 days. Maersk will followup that assessment by implementing appropriate measures to address any identified security gap or weakness.

We have made good progress in improving security, but still have a big job in front of us. Without a doubt, it is a complex and multifaceted endeavor that requires the leadership and coordination of the Federal Government.

The Federal Government must establish and enforce standardized security requirements for each participant and each node in the intermodal transportation process. Without mandatory security standards, the competitive environment makes it commercially impossible for an individual company on its own initiative to impose additional security requirements on customers and suppliers. When establishing security requirements, the Federal Government must be mindful of the impact that such requirements could have on the network performance and strike an appropriate balance. We must be careful that security measures do not cause bottlenecks that reduce network velocity and ultimately disrupt military mobilizations and international commerce.

In closing, Maersk believes that the proposed legislation, if enacted and properly implemented, would result in better management and coordination of security efforts. In particular, Maersk supports standardized cargo documentation requirements; national systems for identification cards and personnel credentialling; uniform standards for container security; coordinated security assistance, plans, and response teams. Improving the security of the intermodal transportation will inevitably have a positive impact on the military cargo moving through commercial networks during a mobilization; therefore, Maersk believes that the proposed legislation is an important step in the right direction.

Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify before you today.

Mr. SHAYS. Thank you very much.

[The prepared statement of Mr. Goulden follows:]

Testimony of

Kenneth C. Gaulden

Vice President of Government Marketing

Maersk Line, Limited

Before the House Subcommittee on

National Security, Veteran Affairs, and International Relations

Washington, DC
July 23, 2002

Mr. Chairman and members of the Subcommittee, it is a pleasure for me to appear before you today to speak about security coordination measures at strategic seaports during mobilization of military cargo. Maersk Line, Limited shares your commitment to ensuring that security measures are in place to protect military personnel and cargo during a mobilization.

By way of background, most of you are probably familiar with the Maersk Sealand name and logo because you see our equipment and personnel in United States ports and on America's highways. Maersk Sealand is the one of the largest providers of global intermodal transportation services in the world. Global intermodal transportation consists of integrating various modes of transport (ocean-going vessels, truck, rail, barge) to move shipping containers loaded with cargo from the shipper's facility to the overseas facility of the designated consignee. To provide such door-to-door service, Maersk Sealand has built and operates an integrated transportation network covering over 100 countries. Our network includes more than 250 ocean-going vessels, numerous terminals on five different continents (including twelve ocean terminals here in the United States, most of which are located at strategic seaports), over 800,000 shipping containers, business relationships with trucking companies and railroads around the world, and sophisticated information management systems to track each shipment from initial order to final delivery.

One of Maersk Sealand's most important customers is the U.S. government, and the Department of Defense in particular. Accordingly, we have one company – Maersk Line, Limited – whose primary mission is to support the U.S. Government transportation requirements in peacetime and in war. For the sake of simplicity, I will refer to Maersk Sealand and Maersk Line, Limited interchangeably as "Maersk." Two of our main business areas with the Department of Defense are: (1) ship ownership and management services; and (2) global intermodal transportation services.

Ship Ownership & Management Services – Maersk owns and/or operates a sizable fleet of ships exclusively for the U.S. military. The fleet includes two ammunition ships, eight large medium speed roll-on roll-off (LMSR) ships, five maritime pre-positioning ships, and twelve TAGOS ships. These ships typically call at seaports controlled by the U.S. military.

Global Intermodal Transportation Services – In addition to providing transportation assets dedicated exclusively to the military, we also provide the military with global intermodal transportation services using our commercial intermodal network. By leveraging existing commercial intermodal networks, the military obtains capabilities in terms of geographic scope, speed, capacity, and efficiency that it could not otherwise obtain. Currently, Maersk transports approximately 30,000 forty-foot equivalent units (FEUs) annually for the Department of Defense, which equates to almost 50 percent of the Department's total intermodal requirements in peacetime.

In addition to providing peacetime support, Maersk also supports the military's mobilization requirements through its participation in the Maritime Security Program and the Voluntary Intermodal Sealift Agreement (VISA) program. Under these programs, Maersk has committed to provide the U.S. military with more intermodal and vessel capacity and capabilities during mobilizations than any other carrier in the world. This commitment is memorialized in pre-negotiated contracts to facilitate a quick and seamless transition from peacetime to contingency operations.

The focus of my testimony here today is to answer the questions posed to me by the Subcommittee in the context of providing global transportation services to the U.S. military, in peacetime and in war, using commercial intermodal networks and assets.

What measures should the federal government take to address the issue of security at seaports?

The federal government needs to take measures that will secure the commercial intermodal transportation networks in which containerized cargo moves into and out of the United States. These measures should provide sufficient security without unduly taxing the intermodal transportation network in terms of costs and operational efficiency.

The federal government should examine security at each transportation node or phase in the context of the entire intermodal transportation process as opposed to examining one node, such as seaports, in isolation. In an integrated transportation network, each entity that participates in the network must be able rely on other network participants to institute necessary security measures. Every government agency and commercial party involved in the transportation of goods has a role to play in maintaining security.

The federal government's role should be establish and enforce standardized security requirements for each participant in the intermodal transportation process. When establishing security requirements, the federal government should be mindful of the impact that such requirements could have on the flow of international trade and strike an appropriate balance.

We fully support Congressional enactment of legislation to improve the security of intermodal transportation networks. The World Shipping Council, of which we are a member, has previously provided Congress with a number of recommendations regarding specific provisions of the House and Senate Bills. While I will not repeat them here, I would like to reiterate Maersk's support of the recommendations made by the World Shipping Council.

What procedures are in place during mobilization to protect military forces and cargo deploying through strategic seaports?

Maersk has a panoply of security systems and measures in place at all times to protect its intermodal network and the cargo moving within that network. Even before security became the hot topic it is today, Maersk's security program was firmly in place with U.S. Customs and the U.S. Coast Guard. Indeed, Maersk is one of the few ocean carriers in the world that has qualified for the *U.S. Customs Super Carrier Initiative*, which had represented the U.S. Custom's most stringent security requirements. Since September 11th, Maersk has worked diligently to harden its existing security systems and procedures (e.g., more vigorous identification checks, greater access control to critical areas, physical security onboard vessels, etc.) Maersk also has been actively engaged with cognizant government agencies and industry groups, both here and abroad, to improve transportation security.

With respect to military cargo during a mobilization, as previously mentioned, Maersk and other U.S. flag carriers participate in the VISA program. The VISA program is the primary mechanism for effectuating a large-scale sealift mobilization of military cargo. Under the VISA program, the U.S. military maintains contracts with U.S. flag carriers that can be activated if and when a large-scale sealift mobilization is required.

The VISA contracts provide a number of provisions that can be implemented to provide additional security to military cargo and to mitigate the operational disruption that a successful terrorist attack might have on the mobilization. These include:

Joint Planning & Advisory Group – The VISA program established a Joint Planning & Advisory Group (JPAG) in which the military and VISA participants can work together to develop and recommend Concepts of Operations (CONOPS) to meet mobilization requirements. VISA participants generally have personal and facility security clearances so that the military can provide the VISA participants with classified information where appropriate. In developing these CONOPS, the military and VISA participants will address what security measures will be implemented to protect military cargo while at the same time allowing for an efficient and effective mobilization.

Flexible Vessel Routing – In coordination with the military, the VISA carrier can provide flexible routing of military cargo during mobilization. For example, military cargo can be routed on a particular land route in the U.S. Cargo may be routed to a particular U.S. port for security reasons or to avoid disruption at a port that was a target of terrorism. On the other hand, cargo may be routed to many different ports to diffuse the concentration of military cargo at any particular port. Vessels carrying military cargo during a mobilization may sail directly to the discharge port or bypass certain intermediate foreign ports to avoid potential threats.

Dedicated Ocean Service – If deemed necessary by the military for operational reasons (including security), a VISA carrier will establish a dedicated ocean service that transports military cargo exclusively between the ports designated by the military. Such a "closed loop" service should be less vulnerable to attack and easier to defend.

Supercargo – At its discretion, the military can choose to place military personnel onboard activated vessels to guard and protect military cargo during the ocean voyage.

Crew – The military will have the discretion to replace any of the crew manning an activated vessel in the event it determines that such person(s) is prejudicial to the interests or endangers the security of the United States.

What procedures have been instituted to develop risk assessments for strategic seaports during a mobilization of troops and equipment?

There are at least two components of developing risk assessments for strategic seaports during a mobilization of troops and equipment. One component is an assessment of the threat (e.g., who, what, when and where). In that regard, Maersk and other commercial carriers must rely largely on the intelligence gathering and analysis capabilities of government agencies to identify and assess threats.

Another component is vulnerability assessment. Here, Maersk is in the process of completing a worldwide self-assessment and gap analysis of its security systems and procedures for its commercial intermodal network. Maersk will follow up that assessment by implementing appropriate measures to address any identified security gap or weakness. This process will undoubtedly result in improved security for military cargo moving through Maersk's intermodal network during peacetime or a mobilization.

In addition, the U.S. military and VISA carriers will work together during a mobilization to assess the specific vulnerabilities on a particular trade route or for particular cargo, and focus on minimizing or eliminating any perceived vulnerabilities. As explained earlier, the U.S. military and the VISA carriers have a number of tools at their disposal to protect military cargo during a mobilization. We anticipate that additional tools will become available as various transportation security initiatives begin to bear fruit.

Since September 11, 2001, what changes have been made concerning how security is managed and coordinated at strategic seaports during mobilization of military forces and cargo?

Overall Security – Maersk has made a number of changes concerning how overall security is managed and coordinated at strategic seaports. Internally, Maersk has established a Global Line Security Council to provide worldwide management and coordination of its security activities. These activities include the hardening of existing security measures and a worldwide self-assessment and gap analysis of Maersk's current security systems and procedures.

Externally, Maersk has intensified its coordination with cognizant government agencies. Maersk has worked closely with the U.S. Coast Guard to implement various security measures commensurate with applicable threat levels. Just last week, Maersk became one of the first carriers to participate in the U.S. Customs Trade Partnership Against Terrorism (C-TPAT) initiative. Overseas, Maersk is working with foreign governments and international organizations on security issues.

While many companies and government agencies have been diligently working to improve security and have made good progress, there is room for improvement. We believe that the work being done by Congress in this area will help improve security management and coordination at strategic seaports and other nodes in commercial intermodal networks.

Military Specific Security – Since September 11th, we have continued to work closely with the U.S. military to institute additional security measures focused on particular military shipments or types of shipments. For example, Maersk has transported over 500 containers to Southeast Asia in support of Operation Enduring Freedom. When planning these shipments with the military, we consider security risks when deciding whether to route the cargo from the south through Pakistan, or from the north through the former Soviet Union. We also evaluate whether additional physical security measures should be taken (such as hiring armed guards to escort the cargo or installing additional steel bars to prevent tampering with the contents of the sealed containers) and implement such measures as appropriate.

How will proposed legislation, H.R. 3983 and S. 1214, assist in coordinating the multitude of agencies involved in port operations during mobilization of military forces and cargo?

Presently, the proposed legislation does not appear to impose any requirements that are specifically aimed at transportation security for the mobilization of military forces and cargo. Maersk would welcome the opportunity actively participate with the military and other government agencies on a transportation security initiative (legislative or otherwise) that focuses on military mobilizations. The VISA program would provide an excellent forum for work in this area with respect to military cargo moving in commercial intermodal transportation networks. During an actual mobilization, the military and VISA carriers will continue to jointly develop and implement CONOPS that satisfy all operational requirements, including security.

As previously stated, Maersk believes that the proposed legislation, if enacted and properly implemented to address the entire intermodal transportation network, would result in better management and coordination of security efforts. The following items are particularly important and beneficial:

- Standardized Cargo Documentation Requirements
- National System for Identification Cards and Personnel Credentialing
- Uniform Standards for Container Security (e.g., seals, locks)
- Coordinated Security Assessments, Plans, and Response Teams.

Improving the security of the intermodal transportation will inevitably have a positive impact on military cargo moving through that network during a mobilization. In short, we believe that the proposed legislation is an important step in the right direction for both commercial and military cargo during peacetime as well as during mobilizations.

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to testify before you today.

Mr. SHAYS. Let me ask what may appear to be somewhat of a facetious question, but it is not intended that way. I'd like to just see where it leads us.

Tell me something hopeful. Tell me something encouraging about our ability to protect our strategic resources at our seaports. I'll throw it open to you first, Mr. Decker, and then to Mr. Goulden.

Mr. DECKER. Mr. Chairman, could I ask for a rephrasing of the question, please?

Mr. SHAYS. Yes.

Mr. DECKER. Thank you.

Mr. SHAYS. I'll preface it by saying as I listened to the testimony I feel like—and as I think of what I've seen in my work chairing this committee, I don't know a lot that I can feel encouraged about in our capabilities to protect vital resources in our ports. Given, in particular, that a lot of the ports have dual use—they really have three. They have military—our harbors do. They have military, they have commercial, and they have recreational uses. I don't feel that we have an infrastructure in place that is particularly good at protecting our facilities. I don't feel we have the manpower. I don't feel we have the coordination yet. I don't think we've done our risk assessment. I don't think that we've developed a strategy. So I started to get a little depressed about it.

Tell me some hopeful things that I can say, "Oh, gosh, this is better than I think."

Mr. DECKER. Sir, I think one of the most hopeful aspects, besides the good work that I think people are trying to do at the different executive agencies at different levels, are the provisions in the Senate Resolution 1214. Really, that legislation, with its counterpart House resolution, which is an amendment to that resolution, really provides for the first time a tremendously top-down-to-the-bottom-level framework that is going to help the national leadership as well as the local officers that are responsible for working port security issues with tools that will allow them to move forward. This will take some time, though, for this to evolve.

If you look at a couple of the major points that were brought up earlier, some of the issues that are being worked on, port vulnerability assessments, this legislation prescribes that there has to be some standards applied and there has to be some consistency with how they are done across the board. Right now that's not the case.

Department of Defense has had a very long program of force protection in which they have come up with a good process for vulnerability assessments, and I was encouraged to hear that DTRA is going to be involved working with the Coast Guard, with the Maritime Administration, and others—MTMC—to work on that. So legislation is part one.

Part two is I think that there are a lot of response-type actions that are positive. The one I mentioned about the Coast Guard with their SWAT-like teams that go out and look at suspicious vessels before they get into a port, that's positive, the studies that are ongoing looking at sea container security issues. But there is a lot a question about are we better today than we were a year ago, you know, independent of September 11th, and I'm not really sure I can answer that, with the work that we've done. I just sort of share your concerns.

Mr. GOULDEN. Your concerns are well placed, but, having said that—and I think everyone recognizes that—the amount of focus today as opposed to prior to September 11th is incredible. You can't go anywhere in our business and not have security be a mainstay portion of it. There are pilots in place, the Customs C-TPAT partnering agreement that I talked about, security.

Mr. SHAYS. You mean pilot programs?

Mr. GOULDEN. Pilot programs in place like the C-TPAT.

Mr. SHAYS. Because you do have pilots at your harbors.

Mr. GOULDEN. At the ports we have pilots. Yes, we do. You got it. Pilot programs. You got it. Security seals, our other pilot programs that are in place. There have been a few more mentioned here.

The industry is thirsty for answers on how to improve the system and how do they participate in the system. There is a growing recognition that cargo plays an important part, and it is the whole intermodal network, not just one node.

Granted, the port is where everything comes in and out of, but knowledge of things away from there which are much more difficult to assess are now being looked at as the long-term solution to offer some protection to the ports.

So I think there is a lot to be hopeful for. We certainly aren't there yet.

Mr. SHAYS. Your company has contracts, as you pointed out, obviously, with the military to ship. Are all your ships dedicated to military transportation, or is it—do you sometimes—do you have some ships just totally dedicated and other ships that are used where needed?

Mr. GOULDEN. Correct. We have a group of vessels where we either own those vessels and charter them and manage them for the U.S. Government or we manage U.S. Government vessels for them, and those are totally dedicated to the Department of Defense and the work that the Department of Defense does.

Mr. SHAYS. So any transportation of military hardware is on a dedicated ship?

Mr. GOULDEN. There is a set that's done that way. We also have 23 vessels that we operate in our commercial fleet, so of 250 worldwide vessels, 23 of those would be in commercial operation off of U.S. shores integrated into that commercial fleet. By and large, the majority of the cargo on those ships is commercial cargo moving in and out of foreign commerce of the United States through U.S. ports.

We also move about 30,000 40-foot equivalents for the U.S. military in peacetime in foreign commerce on those same U.S.-flagged vessels, which are U.S. flagged, crewed by U.S. crew members and U.S. citizens, and operated by us in our fleets. They are also documented U.S.-flagged vessels.

Mr. SHAYS. Thank you.

Mr. Decker, General Privratsky's testimony stated that the Military Traffic Management Command coordinates with other organizations and shares information. Your study and testimony implies there is need for significant improvement, so I'd like to ask how should the MTMC improve coordination of force protection measures.

Mr. DECKER. Mr. Chairman, if you will allow me, I'd like to have my colleague, Mr. Kirschbaum——

Mr. SHAYS. I'd be delighted to have him respond.

Mr. DECKER [continuing]. Provide a comment on that, if you will.

Mr. SHAYS. The question is, is he delighted to respond? [Laughter.]

Do you want me to repeat the question?

Mr. KIRSCHBAUM. No, sir, Mr. Chairman. Thank you. By and large, at the ports we visited—the point the general made about the coordination mechanisms at the Port Readiness Committees and the role that his command plays, from our view is fairly systematic. They do have processes in place and they follow them fairly closely and they are most assuredly dedicated individuals.

Where the variance comes in is in the stages of the deployment process from the fort to the port, as Mr. Decker alluded to earlier, where there are several phases at which force protection concerns are critical, but the actual transport is changed. It is changed hands from the military installation, from road or rail movement, and then at some point at the port when the military equipment changes over. At the port, itself, that Port Readiness Committee structure is in place where you have MTMC coordinating with the Coast Guard, with local military commanders. That same level of planning, of assessments, and of coordinated force protection measures cannot be traced to the same level at all stages of that deployment. It's when you step back to that overall view you see that there's a potential that the same level of planning has not been done throughout the entire process. That's the difference.

Mr. SHAYS. Thank you.

Mr. Goulden, when military hardware, equipment, is loaded on non-DOD ships—in other words, on one of your ships—what kind of security arrangements are made? Do you carry any military flag? Do you have military personnel on board? Are you treated like a commercial ship or like a military ship?

Mr. GOULDEN. We're treated as a commercial ship. The cargo that comes on into the port and loaded for DOD onto our vessels would be treated as the same unless the U.S. military asks for special treatment. Our contracts enable them to say that they could have a super cargo, that they would want someone to watch that cargo all the way through from loading to destination and then hand it off at the other end. That assessment of their cargo and how they want it handled is done by theirs, and our contractual relationship enables us to implement the terms that they would like.

Mr. SHAYS. Thank you. Is there any question that any of the three of you feel that we need to put on the record and want to ask yourself the question and answer it? Is there a question that you think we need to put on the record?

Mr. GOULDEN. Not from me.

Mr. SHAYS. Mr. Decker.

Mr. DECKER. Mr. Chairman, I would like to just pursue that question you asked.

Mr. SHAYS. Sure.

Mr. DECKER. And with the help of our distinguished colleague, perhaps illuminate more on the issue.

Mr. SHAYS. Sure.

Mr. DECKER. A concern that we raised had to do with the military equipment being transported on ships of foreign flag with crews from other countries.

Mr. SHAYS. Let me be clear. So these are—your ships would not necessarily be U.S.-flagged ships?

Mr. GOULDEN. We would move military cargo that was booked with us on our U.S.-flagged vessels. In the event no U.S.-flagged vessel was available, a determination of non-availability would be made, then the military has the right to authorize the cargo to be booked on one of our foreign-flagged vessels.

Mr. SHAYS. Sorry, Mr. Decker. I just wanted to ask him.

Mr. DECKER. No. In fact, that's exactly where I was headed with the question. When we did some of our site work, we looked at the ship manifests, the cargo on nine ships of different flags, and also the crew manifest, the crew list. And what we noted—and these were in support of military operations overseas, not a mobilization but ongoing operations—the ships, by and large, except for one, was of a foreign—all foreign flagged. Now, some is I think flag of convenience for other reasons, but several were owned by foreign countries and therefore—and then flagged in different countries. Crews were totally from other countries. Yet, on these ships during the missions we looked at you had Bradley fighting vehicles, 155 millimeter howitzers, Black Hawk helicopters, machine guns, night vision goggles, nuclear biological chemical defense equipment, and it just goes on—communications equipment.

Mr. SHAYS. So you would draw from that what?

Mr. DECKER. Well, a concern that perhaps—and maybe the risk is acceptable, but do we know everything we need to about the ships and the crews that are not under U.S. flag or U.S. control, that the risk is acceptable when we move high-value, very sensitive, important equipment.

I thought my colleague would be able to, from his perspective, knowing the business, might be able to share some insight on that.

Mr. SHAYS. Would you care to respond to that?

Mr. GOULDEN. I'm not familiar with the statistics, so I don't know if these were spot charters or liner operations or whatever, but I do know that the Military Sealift Command routinely charters vessels that are foreign flagged once they've made a determination that there are no U.S.-flagged vessels available.

Mr. SHAYS. And do they do that through you or do they do it independently?

Mr. GOULDEN. No, they do it independently. They do a request for bid and people put in proposals.

Mr. SHAYS. And how much of the non-military-transported goods do you think your company does? Do you do 10 percent of it, 50 percent of it?

Mr. GOULDEN. In what we would call "liner traffic," cargo that moves within a specific contract called the "universal service contract 03," which is managed by the Military Traffic Management Command, on a global basis in foreign commerce we probably handle somewhere between 45 and 50 percent of the cargo.

Mr. SHAYS. You had a lot of explanation before you got to that number.

Mr. GOULDEN. Well, you don't want to confuse it——

Mr. SHAYS. Yes, I understand.

Mr. GOULDEN [continuing]. With domestic cargo and other cargos.

Mr. SHAYS. So you do almost half?

Mr. GOULDEN. Yes, approximately half. Correct.

Mr. SHAYS. So can I infer that the other half is going on non-U.S.-flagged ships?

Mr. GOULDEN. No, you cannot.

Mr. SHAYS. OK.

Mr. GOULDEN. The other half would go on competitors that are U.S. flag operators with U.S. citizen crews, similar companies just like my own—American President Lines, Lykes Lines, Farrell, Central Gulf Waterman—make sure I get them all in there, because they won't be happy with me if I don't. But they all participate in the same contract and would handle the rest of the cargo.

Mr. SHAYS. Gentlemen, is there anything else we need to put on the record?

[No response.]

Mr. SHAYS. Then I'd like to thank you. I appreciate your testimony. I appreciate your putting this on the record. I think this is clearly a work in process and a new area for this committee, so we will be getting into it in a lot more depth.

Thank you.

This hearing is adjourned.

Mr. DECKER. Thank you.

Mr. GOULDEN. Thank you, sir.

[Whereupon, at 12:20 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]