U.S. House of Representatives
Committee on Transportation and Infrastructure
Washington, DC 20515

John L. Mica
Chairman

Nick J. Rahall, II
Ranking Member

James W. Coon II, Chief of Staff

James H. Zoia, Democrat Chief of Staff

September 7, 2012

MEMORANDUM

TO: Members, Subcommittee on Coast Guard and Maritime Transportation

FROM: Staff, Subcommittee on Coast Guard and Maritime Transportation

RE: Hearing on "Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer?"

PURPOSE

On September 11, 2012, at 9:30 a.m., in 2212 Rayburn House Office Building, the Subcommittee on Coast Guard and Maritime Transportation will hold a hearing to review the Coast Guard's implementation of the Maritime Transportation Security Act of 2002 (MTSA) since its passage 10 years ago and identify what improvements still need to be made to enhance the security of our nation's maritime transportation system.

BACKGROUND

The Maritime Transportation Security Act of 2002

Following the terrorist attacks of September 11, 2001, the Subcommittee developed legislation to improve the security of the nation's ports and waterways. On November 25, 2002, S. 1214, the Maritime Transportation Security Act of 2002 (P.L 107-295) was signed into law. MTSA established a framework to improve the security of the nation's ports, waterways, and vessels from potential terrorist attacks. MTSA was codified as Chapter 701, Port Security, of title 46, United States Code.

Responsibility for carrying out the provisions of MTSA was vested in the Department of Homeland Security (DHS) and its component agencies, namely the Coast Guard, Customs and Border Patrol (CBP), and the Transportation Security Administration (TSA). On October 22, 2003, the Coast Guard issued interim final regulations (RIN1625-AA43, RIN 1625-AA46) implementing most of

MTSA's provisions. Final regulations implementing other provisions of MTSA were issued from 2004 to 2010. Final regulations governing the deployment of Transportation Worker Identification Credential (TWIC) electronic readers remain to be issued (see below).

MTSA regulates U.S. flagged vessels and domestic facilities. Foreign flagged vessels and facilities are subject to the International Maritime Organization's (IMO) International Ship and Port Facility Security Code (ISPS), which was ratified shortly after MTSA's passage. The ISPS Code was implemented to provide a standardized international framework for foreign port facilities and vessels to assess vulnerabilities and improve security. Its provisions are substantially similar to the implementing regulations of MTSA. The Coast Guard is the primary federal agency responsible for enforcing ISPS regulations on foreign flagged vessels operating in U.S. waters. Since inception of the ISPS Code in 2004, over 300 foreign vessels have been detained, expelled, or denied entry to the U.S. by the Coast Guard under the auspices of the ISPS Code.

Several subsequent acts of Congress have made amendments to MTSA, most notably the Security and Accountability For Every (SAFE) Port Act of 2006 (P.L. 109-347) and the Coast Guard Authorization Act of 2010 (P.L. 111-281). This memo will focus primarily on the Coast Guard's role in implementing the major provisions of MTSA.

Vulnerability Assessments:

MTSA requires the Secretary of Homeland Security (Secretary) to conduct security assessments of vessel types, such as tankers carrying oil or natural gas, and port facilities operating in the U.S. which pose "a high risk of being involved in a transportation security incident." The Coast Guard completed vulnerability assessments of 55 strategic port areas in January 2004. The assessments are updated every 5 five years by the Coast Guard.

Maritime Transportation Security Plans:

In addition to the vulnerability assessments conducted by the Coast Guard, MTSA requires certain U.S. vessels and port facilities to conduct their own vulnerability assessments and develop individual security plans. These plans must: outline passenger, vehicle, and baggage screening procedures; identify an individual responsible for security; designate restricted areas within the facility or vessel; explain personnel identification procedures and access control measures; describe what equipment and infrastructure will be installed to improve security; and discuss other security procedures. The plan must be updated every five years. The Coast Guard is responsible for the review, approval, and enforcement of these security plans. There are currently 3,161 facilities and 14,533 vessels operating under Coast Guard approved security plans.

MTSA requires the Secretary to prepare a National Maritime Security Plan (NMSP) to establish terrorist incident response procedures and coordinate the duties and responsibilities of relevant federal departments and agencies. The National Strategy for Maritime Security (NSMS) and its eight supporting implementation plans released in September 2005 satisfies this requirement. Additional information on NSMS and its implementing plans may be found at: http://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html.

MTSA also requires certain port areas to develop Area Maritime Security Plans (AMSP) which identify high risk facilities and infrastructure in the port area, establish response measures and coordinate the responsibilities of area response agencies, and identify salvage procedures to restore operations after an incident. AMSPs are developed and periodically updated by the Coast Guard Captain of the Port in consultation with members of the Area Maritime Security Committees. These committees include stakeholders from the local maritime industry, the boating public, and other relevant state and local agencies.

Transportation Security Cards:

MTSA requires the Secretary to prescribe regulations requiring individuals needing unescorted access to secure areas of certain vessels and maritime facilities to be issued a biometric identification. TSA developed the Transportation Worker Identification Credential, in consultation with the Coast Guard, to meet these requirements. The goal of the TWIC program is to develop a biometric credential that is interoperable across transportation modes and compatible with existing independent access control systems. Individuals requiring access to secure areas of MTSA regulated facilities or U.S flagged vessels are required to obtain a TWIC. To date, over 2.1 million workers have been issued credentials.

Section 104 of the SAFE Port Act requires the Secretary to conduct a pilot program to test technology to read TWIC and its biometric identification information and established a deadline of April 13, 2009 to issue final rules for the deployment of TWIC readers. The TSA did not complete the pilot program and issue its program report until February 27, 2012. Shortly thereafter, the Coast Guard began the process of developing a Notice of Proposed Rulemaking (NPRM) for the deployment of TWIC readers. The Coast Guard now expects to publish the NPRM in the fall of 2012. The implementation of a final rule could take up to a year after the NPRM is published. A cost estimate of compliance with the reader requirement has not been prepared. Without the readers in place, TWICs are used as a flash pass as workers enter secure areas of facilities and vessels. As a result, the biometrics are not read and identities are not easily verified. However, the Coast Guard uses hand held readers to check the validity of TWICs during inspections of port facilities and U.S.-flagged vessels.

Port Security Grants:

The costs incurred by port authorities, facility operators, and state and local government agencies seeking to comply with MTSA requirements are vast. The Port Security Grant Program (PSGP), authorized under MTSA, provides matching grants to these entities to assist in the compliance with facility security plans including costs associated with security personnel, acquisition and operation of security equipment and infrastructure, and certain other security related activities. Since fiscal year 2002, over $2 billion in PSGP funding has been made available to state, local, and private entities to improve port security. In the fiscal year 2013 budget request, the President proposes to combine PSPG and 15 other security grant programs into a single National Preparedness Grant Program.

Foreign Port Assessments:

MTSA requires the Secretary to assess the effectiveness of anti-terrorism measures in the foreign ports. In 2004, the Coast Guard established the International Port Security (IPS) program. Since the beginning of the IPS program, the Service has sent personnel to assess the security of 1,029 foreign port facilities and determine compliance with the ISPS code. The Coast Guard uses these visits to help create a threat matrix for vessels calling on U.S. ports. Vessels coming from foreign port facilities with security vulnerabilities identified under the IPS program score higher on the threat matrix and are targeted for boarding, denial of entry, or other actions upon arrival in U.S. waters. The Coast Guard currently maintains a list of 16 countries which are not maintaining effective anti-terrorism measures:

1. Cambodia (except certain ports)
2. Cameroon (except certain ports)
3. Comoros
4. Cuba
5. Cote d'Ivoire
6. Equatorial Guinea (except certain ports)
7. Guinea- Bissau
8. Indonesia (except certain ports)
9. Iran
10. Liberia (except certain ports)
11. Madagascar (except certain ports)
12. Sao Tome and Principe
13. Syria
14. Timor-Leste
15. Venezuela
16. Yemen

Deployable, Specialized Forces:

MTSA mandates the creation of a deployable maritime security teams to enhance domestic maritime security. The Coast Guard's Maritime Safety and Security Teams (MSST) and Maritime Security Response Team (MSRT) satisfy this requirement.

Based in eleven ports nationwide, MSSTs are forces capable of rapid deployment in response to changing threat conditions and evolving maritime security needs. MSST duties include enforcing security zones, protecting military out-loads, ensuring maritime security during major marine events, augmenting shore-side security at waterfront facilities, and detecting weapons of mass destruction. In fiscal year 2011, the Coast Guard decommissioned its MSST based in Anchorage, Alaska.

The MSRT, which is based in Chesapeake, Virginia, consists of only one deployable team with a helicopter. The MSRT is a more highly specialized resource than the MSSTs and is used for more advanced counterterrorism operations. The primary duties of the MSRT are to deny terrorist acts, take security actions against non-compliant actors, perform tactical facility entry and enforcement, participate in port level counterterrorism exercises, and educate other forces on counterterrorism procedures.

Automatic Identification Systems:

Automatic Identification System (AIS) is an internationally adopted Very High Frequency (VHF)-based, short-range communication system which provides a means for vessels to electronically exchange data, including identification, position, course, and speed, with other

nearby vessels and shore-based AIS receivers. Depending on signal strength, weather, geography, and receiver capability, AIS signals can generally be received up to 50 miles away. MTSA requires certain commercial vessels operating in certain U.S. waters to carry AIS. In October 2003, the Coast Guard finalized its rule implementing the AIS carriage requirements (RIN 1625-AA67).

On December 16, 2008, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) (RIN 1625-AA99) to amend the current AIS regulations to expand AIS carriage requirements to vessels operating in all U.S. navigable waters, and require AIS carriage for additional commercial vessels, including certain fishing and towing vessels. The NPRM would more than double the number of vessels currently tracked by the Service. The final rule is still under development by the Coast Guard.

Long-range Vessel Tracking System:

MTSA requires the Coast Guard to establish a long range tracking system to receive information on vessels operating beyond the scope of the existing and planned AIS system. Long Range Identification and Tracking (LRIT) is a worldwide, satellite-based automated tracking system that extends tracking capabilities up to 2000 nautical miles offshore. LRIT is a secure system in which data transmissions are made in a protected format to data centers which distribute them to countries permitted to have the information. The LRIT system provides information on vessel identity and position every six hours. It became operational on December 31, 2008. The Coast Guard collects and distributes vessel position data to participating countries in the LRIT system.

Penalties:

Individuals found in violation of MTSA or its implementing regulations are subject to civil penalties of not more than $25,000 per day. Any vessel operated in violation of MTSA or its implementing regulations can be held liable in rem. Finally, the Coast Guard may prevent port facilities from operating and revoke or suspend the clearance of a vessel (prohibiting it from operating in U.S. waters) for violations of MTSA or its implementing regulations. Since 2004, the Coast Guard has prevented 82 facilities and 528 vessels from operating due to MTSA violations.

Recent Findings of the Government Accountability Office

Through reports and testimony before Congress over the last several years, the Government Accountability Office (GAO) has highlighted areas of MTSA implementation that are incomplete or unsatisfactory. Areas of concern include the following:

TWIC:

On May 10, 2011, the GAO released a report entitled *TWIC: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Directives* (GAO-11-657). To test the effectiveness of the TWIC program, GAO reviewed program documentation, visited four

TWIC enrollment centers, and conducted covert tests at several selected U.S. ports. During covert tests of TWIC use at several selected ports, GAO investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases. The Coast Guard still has not published a final rule for the deployment of TWIC readers. Without readers in place, facility operators cannot easily verify the identity of workers seeking entrance into restricted areas.

Foreign Seafarer Identification:

In a 2011 report to Congress entitled *Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened* (GAO 11-195), the GAO raised concerns about the ability of CBP and the Coast Guard to verify identity and immigration as a part of its onboard inspections of cargo vessels. DHS currently lacks the technology needed to conduct an onboard electronic verification, thus limiting the agencies' abilities to detect fraudulent documents while onboard a vessel.

Foreign Port Assessments:

On July 21, 2010, GAO testified before the Senate Committee on Commerce, Science, and Transportation (GAO 10-940T) and noted two hurdles facing the Coast Guard's International Port Security Program. The first was reluctance on the part of foreign port nations to allow Coast Guard officials to frequently observe their port operations. The other issue was a lack of resources to directly assist foreign ports with their efforts to enhance security measures.

WITNESSES

Rear Admiral Joseph Servidio
Assistant Commandant for Preparedness
United States Coast Guard

Mr. Stephen Caldwell
Director
Homeland Security and Justice Issues
Government Accountability Office

Ms. Beth Rooney
Manager of Port Security
Port Authority of New York & New Jersey
Testifying on behalf of:
American Association of Port Authorities

Mr. Chris Koch
President & CEO
World Shipping Council