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

Bill Shuster
Chairman

Christopher P. Bertram, Staff Director

Peter A. DeFazio
Ranking Member

Katherine W. Dedrick, Democratic Staff Director

July 1, 2016

SUMMARY OF SUBJECT MATTER

TO: Members, Subcommittee on Coast Guard and Maritime Transportation
FROM: Staff, Subcommittee on Coast Guard and Maritime Transportation and the Subcommittee on Border and Maritime Security
RE: Joint Hearing on "An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security and Smuggling Risks in the U.S."

PURPOSE

The Subcommittee on Coast Guard and Maritime Transportation and the Subcommittee on Border and Maritime Security will meet on July 7, 2016 at 10:00 a.m. in 2167 Rayburn House Office Building, to hold a joint hearing to examine the efforts of the Department of Homeland Security to prevent nuclear smuggling in United States Ports (U.S.). The Subcommittees will hear from the U.S. Coast Guard, the Domestic Nuclear Detection Office, U.S. Customs and Border Protection, National Nuclear Security Administration, the U.S. Government Accountability Office, Los Alamos National Laboratories, the Maryland Port Administration, and the Lake Carriers' Association.

BACKGROUND

The U.S. maritime border includes 95,000 miles of open shoreline, 361 ports and an Exclusive Economic Zone that spans 4.5 million square statute miles. These ports connect to 152,000 miles of railways, 460,000 miles of underground pipelines and 45,000 miles of interstate highways. The U.S. relies on ocean transportation for 95 percent of cargo tonnage that moves in and out of the country. U.S. Department of Transportation (DOT) data shows 8,588 commercial vessels made 82,044 port calls in 2015 and 41.6 percent of U.S. foreign trade (by value) was moved by vessel. U.S. foreign trade by vessel was estimated at $1,562.5 billion in 2015, according to the U.S. Census Bureau.

Small Vessel Threats

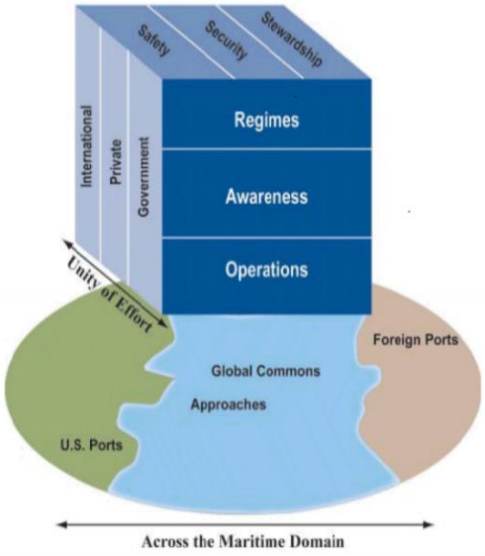
The global Maritime Transportation System (MTS) is an interconnected system of waterways, ports, terminals, intermodal connections, vessels, people, support service industries

and users spanning the domestic and international public and private sectors. In the U.S., in addition to large commercial vessels, the MTS includes approximately 11.8 million registered U.S. recreational vessels and perhaps an additional four million unregistered recreational boaters, 82,000 fishing vessels, and 100,000 other commercial small vessels. These vessels generally fall under the category of small vessels which are characterized as any watercraft regardless of method of propulsion, less than 300 gross tons. They include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other commercial vessels involved in foreign or U.S. voyages. The small vessel community comprises a large and diverse group of boat operators with varying levels of professional and recreational training. These vessels share waterways with commercial and military traffic, and operate in the vicinity of critical infrastructure, including bridges and waterfront facilities such as nuclear and petrochemical plants. Boaters on U.S. waterways present a unique challenge for law enforcement to detect and distinguish between legitimate vessel operators and those engaged in illicit activities such as smuggling.

In April 2008, the Department of Homeland Security (DHS) National Small Vessel Security Strategy *(Strategy)* was developed to address potential security and safety risks from small vessels. It was intended to identify the potential for commercial or recreational small vessels to be used to smuggle terrorists or weapons into the United States, as a stand-off weapon platform, or as a direct attack method to deliver a water-borne improvised explosive device (WBIED).

The overarching goals of the *Strategy* are to:

1. Enhance maritime security and safety based on a coherent framework with a layered, innovative approach;
2. Develop and leverage a strong partnership with the small vessel community and public and private sectors in order to enhance maritime domain awareness;
3. Leverage technology to enhance the ability to detect, infer intent, and when necessary, interdict small vessels that pose a maritime security threat; and
4. Enhance cooperation among international, federal, state, local, and tribal partners and the private sector, and in coordination with the Department of State and other relevant federal departments, agencies, and international partners.



Graphic on Maritime Governance from DHS

The *Strategy* focuses on reducing potential security and safety risks from small vessels through the adoption and implementation of a coherent system of regimes (or rule sets, to describe the desired state of the domain), awareness and security operations that strike the proper balance between fundamental freedoms, adequate security and continued economic stability. Based on the size and complexity of the maritime domain, DHS has chosen a risk-based decision making process which relies on multi-layered system that includes international, national, state, local, tribal, and industry partners.

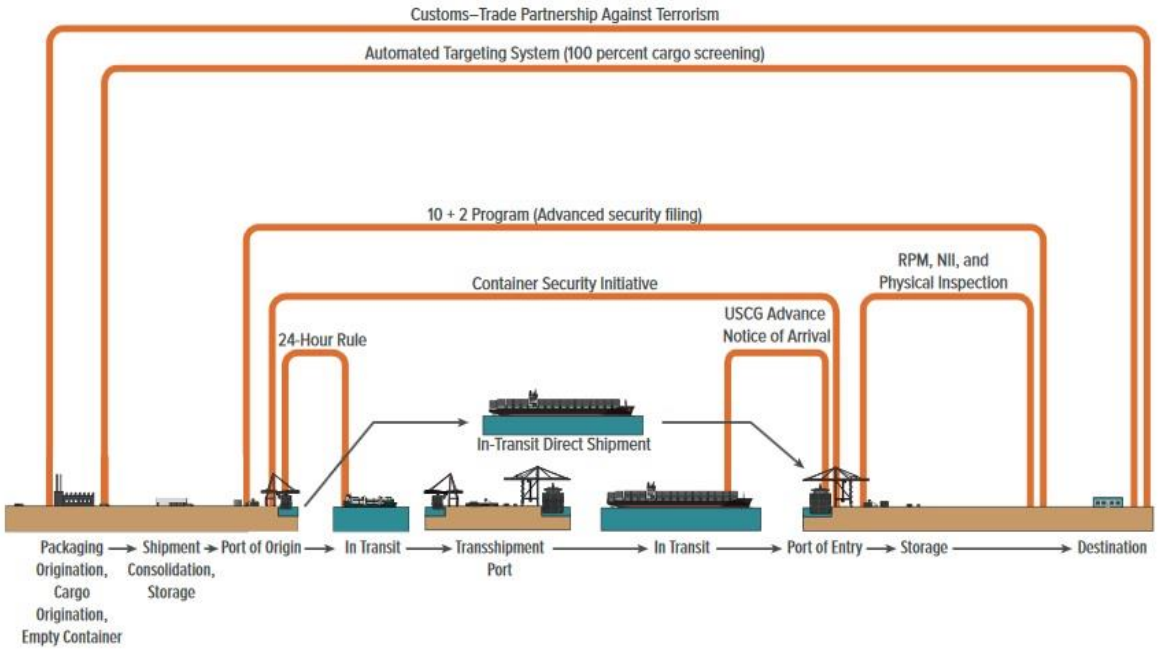
The DHS Small Vessel Security Implementation Plan (*Plan)* was developed as a roadmap for meeting the goals and objectives of the *Strategy* and is intended as a guidance document not a

resourcing document. It defines the goals and objectives of the *Strategy* and outlines ongoing and contemplated federal efforts of DHS components and other partners including Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms & Explosives (BATF), and Department of Defense (DOD), to thwart threats to the homeland through the maritime domain. Development of the *Plan* was initiated by a national Small Vessel Security Summit in 2007 and builds upon input from federal, state, local and tribal authorities to improve Maritime Domain Awareness (MDA). In January 2011, DHS published "Small Vessel Security Implementation Plan Report to the Public." The *Plan* itself is designated Sensitive Security Information, with distribution only to pre-cleared stakeholders (e.g., members of the Area Maritime Security Committees).

As envisioned in the *Strategy*, the *Plan* uses a layered approach to thwart adversaries by increasing the likelihood of detection through a myriad of operational techniques. This approach is designed to be flexible and to be implemented at the federal, state, and local levels to manage specific risks related to maritime terrorism, crime, security, and safety in general.

Container Security

DHS uses a multilayered and risk based security approach that extends beyond the domestic border and ports. Several agencies within the DHS are involved in monitoring threats to the U.S. global supply chain and the movement of goods and materials into and out of the U.S. According to DHS, its security measures take place at different locations, at different times, and are implemented by different organizations based on their jurisdiction. The following Congressional Budget Office (CBO) graphic shows security approaches for containers.



Source: Congressional Budget Office, using data from Customs and Border Protection (CBP).

NII = nonintrusive imaging; RPM = radiation portal monitor; USCG = U.S. Coast Guard.

U.S. Customs and Border Protection (CBP) has primary federal responsibility to ensure that all imports and exports comply with U.S. laws and regulations. CBP works to balance the three overarching U.S. import policies: 1) trade facilitation; 2) enforcement of trade laws; and 3) import security. CBP initiatives focus on the goal of checking the security of cargo before it reaches the U.S. Additionally, CBP uses a layered defense-in-depth system to counter nuclear and other threats to U.S. ports. The layered defense-in-depth system is used to scan all containers for radiation and images about five percent of them based on CBP's risk assessment for all types of threats.

The U.S. Coast Guard (USCG) has primary responsibility for the protection of life and property at sea, as well as the enforcement of all applicable federal laws on, under, and over the highs seas and U.S. waters. The USCG also coordinates all maritime security planning and is responsible for the security of U.S. ports, harbors, waterways, vessels and waterfront facilities.

The Government Accountability Office's (GAO) 2010 report entitled, *Maritime Security DHS Progress and Challenges in Key Areas of Port Security*, notes DHS and its agencies have strengthened risk management decisions through continually evolving risk assessment tools. DHS and CBP have taken various actions to enhance maritime container security. The USCG has initiated similar actions for port security.

The USCG requires all vessels to provide notice of arrival (NOA) to any U.S. port 96 hours in advance, an increase from the previous NOA requirement of 24 hours. In addition, the notice must now include a listing of all persons on board, crew and passengers, with date of birth, nationality, along with the appropriate passport or mariner's document number. The notice must also include the vessel name, country of registry, call sign, official number, the registered owner of the vessel, the operator, the name of the classification society, a general description of the cargo, and the date of departure from the last port along with that port's name.

The USCG uses the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code in its International Port Security Program. The ISPS Code is a global bench mark that measures the effectiveness of a country's counterterrorism measures at a port. USCG personnel visit foreign ports to determine compliance with ISPS. However, the 2010 GAO report states that some countries have been reluctant to allow the USCG to conduct visits at their ports due to concerns over sovereignty. Reciprocal arrangements and visits between the USCG and foreign trade partners have helped gain cooperation. Vessels subject to ISPS Code must maintain their security systems not only in port, but also in transit.

Per the Trade Act of 2002 (P.L. 107-210), cargo container manifests are required to be submitted to CBP 24 hours before shipping containers are loaded at a foreign port onto a U.S.-bound vessel. Other information collected by CBP, per the SAFE Port Act, is commonly referred to as "10+2" shipper information. This information includes 10 elements provided from importers (importer record number, consignee number, seller name and address, buyer name and address, ship-to party name and address, manufacturer name and address, country of origin, Harmonized Tariff Schedule, container location, consolidator (stuffer) name and address) and two elements provided from ocean carriers (vessel stow plan and daily messages with information about container status changes). All of this data is sent to the CBP National Targeting Center – Cargo (NTC-C) in Herndon, VA. CBP uses the data to conduct risk-based

targeting through its Automated Targeting System (ATS), which is a mathematical model that uses weighted rules and algorithms to assign a risk score to arriving cargo shipments. ATS is a decision support tool CBP uses to compare traveler, cargo, and conveyance information against law enforcement intelligence and other data. Using this method, NTC-C screens 100 percent of shipping container and vessel manifest data to determine what shipping containers are high-risk.

CBP runs two voluntary programs – the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) – which were codified in the SAFE Port Act (6 U.S.C. 961). Under C-TPAT, partnerships are established with importers, carriers, brokers, warehouse operators and manufacturers to improve security along the entire supply chain. CBP, along with its C-TPAT partners, examine where cargo originate and assess the physical security and integrity of the foreign suppliers, the background of the personnel involved with the transaction, and the means by which goods are transported to the U.S. As of September 2014, C-TPAT had 10,834 program participants. In June 2014, C-TPAT officials signed a mutual recognition arrangement with Israel's Authorized Economic Operator (AEO) program to further secure and facilitate global cargo trade and allow members of the two programs fewer cargo exams and a faster validation process. The U.S. has similar C-TPAT arrangements with New Zealand, Canada, Japan, Korea, Jordan, the European Union, and Taiwan and is working on C-TPAT arrangements with Mexico, China, India, and Brazil.

The goal of the CSI is to reduce the vulnerability of shipping containers being used to smuggle terrorists or terrorist weapons while accommodating the need for efficiency in global commerce. CBP initially focused implementation of CSI at the 60 largest foreign seaports responsible for shipping the greatest number of shipping containers to the U.S. Ships departing these ports carry approximately 80 percent of all U.S. incoming containerized cargo. CBP reports NTC-C provides targeting support for these 60 overseas CSI locations. In cooperation with the host countries, CBP reported in 2013 that it reviewed 11,228,203 bills of lading and conducted 103,999 examinations of high-risk cargo. Since 2014, DHS has initiated new CSI operations at Port of Aqaba, Jordan, and finalized agreements with the Government of the People's Republic of China to add two additional ports to the existing CSI arrangement (see appendix for additional information on container scanning).

CBP uses non-intrusive technology for cargo entering and leaving U.S. ports. Radiation Portal Monitors (RPMs), installed by the DHS, Domestic Nuclear Detection Office (DNDO) and CBP, are capable of detecting radiation emanating from nuclear devices, dirty bombs, special nuclear materials, natural sources and isotopes commonly used in medicine and industry. "Portal technology" can detect even the weakest radiation and then use sophisticated computer software to specifically identify the source. Any cargo container that triggers an alarm is set aside for more scanning or inspections. Radiological readings are sent to Laboratories and Scientific Services when further adjudication (the process to identify the type or nature of the material and assess the potential threat) is needed. CBP officers also carry radiation isotope identification devices (RIID) which can identify the radiation source, which can include potentially dangerous materials (e.g., plutonium), or benign materials (e.g., kitty litter and granite).

The DNDO has a mission to counter the risk of nuclear terrorism in the U.S. by continuously improving capabilities to deter, detect, respond to, and attribute attacks, in coordination with domestic (federal agencies, state, tribal, and local governments) and

international (foreign governments) partners. DNDO works with federal partners – Departments of Defense, Energy, Justice, and State, the Intelligence Community and the Nuclear Regulatory Commission – to develop the Global Nuclear Domestic Architecture (GNDA). GNDA is a multi-layered, world-wide network that combines 74 independent federal programs, projects, or activities to detect and interdict nuclear smuggling in foreign countries, at the U.S. border, and within the U.S. It includes sensors, telecommunications, and personnel, along with supporting information exchanges, programs, and protocols. These tools serve collectively to detect, analyze, and report on nuclear and radiological materials that are out of regulatory control.

DNDO works with its federal and non-federal partners to determine gaps in the GNDA and implements coordinated research programs to develop new technologies and protocols to address those gaps. End users of the technologies developed include CBP, USCG, Transportation Security Administration, and state, local, and tribal law enforcement agencies. DNDO is made up of seven Directorates. DNDO's Transformational and Applied Research (TAR) Directorate determines what research initiatives to prioritize and fund. During fiscal years 2008-2013, DNDO obligated roughly $350 million for 189 research and development projects, of which approximately $103 million went to 48 projects focused on detecting shielded nuclear material.

WITNESS LIST

Panel I

Rear Admiral Linda L. Fagan
Deputy Commandant for Operations, Policy, and Capabilities
United States Coast Guard

Dr. Wayne Brasure
Acting Director
Domestic Nuclear Detection Office

Mr. Todd C. Owen
Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

Ms. Anne Harrington
Deputy Administrator
Defense Nuclear Nonproliferation
National Nuclear Security Administration

Panel II

Ms. Jennifer Grover
Director, Homeland Security and Justice Issues
Government Accountability Office

Dr. Gregory H. Canavan
Senior Fellow
Los Alamos National Laboratories

Mr. David A. Espie
Director of Security
Maryland Port Administration
Port of Baltimore

Mr. James H.I. Weakley
President
Lake Carriers' Association

APPENDIX

100 Percent Container Scanning

The SAFE Port Act (6 U.S.C. 982), as amended by the 9/11 Commission Act, required 100 percent scanning of U.S.-bound shipping containers by 2012. GAO noted in its June 22, 2015, report entitled *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security* that 100 percent scanning had not been achieved and the feasibility of 100 percent scanning remained unproven. The June 2015 GAO report referred to a 2012 CBO estimate which determined that implementation of 100 percent scanning would cost an average of $8 million per shipping lane and total $16.8 billion for all U.S.-bound containers. GAO also noted that most NII scanning of shipping containers occurs in U.S. ports, not at foreign ports.

Under the SAFE Port Act the DHS Secretary can issue two-year extensions for foreign ports that are unable to meet the 100 percent scanning requirement. Two-year extensions for all ports were made in May 2012, in May 2014, and most recently by Secretary Johnson on May 2, 2016. Secretary Johnson noted in his 2014 letter to Congress that DHS's ability to fully comply with 100 percent scanning is highly improbable.

On May 2, 2016, Secretary Johnson issued a Request for Information (RFI) in an effort to find information, recommendations, or solutions that would allow the DHS to reach its mandate of "100 percent overseas scanning" of cargo to protect the U.S. against radiological and nuclear threats. The scope of the RFI includes containerized and non-containerized maritime cargo departing foreign seaports and bound for the U.S. Both technical and non-technical approaches are being sought and should support the following outcomes: increase in the amount of U.S.-bound maritime cargo scanned; improve global radiological/nuclear detection capability and capacity; and reduce nuclear and other radioactive materials out of regulatory control in the global maritime shipping environment. The submission deadline was June 6, 2016.