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

Bill Shuster
Chairman

Peter A. DeFazio
Ranking Member

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

October 23, 2015

SUMMARY OF SUBJECT MATTER

TO: Members, Subcommittee on Coast Guard and Maritime Transportation
FROM: Staff, Subcommittee on Coast Guard and Maritime Transportation
RE: Coast Guard hearing on "The Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port"

PURPOSE

On October 27, 2015, at 10:00 a.m., in 2167 Rayburn House Office Building, the Subcommittee on Coast Guard and Maritime Transportation will hold a hearing on the Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port. The Subcommittee will hear from the U.S. Coast Guard, the Domestic Nuclear Detection Office, U.S. Customs and Border Protection, the U.S. Government Accountability Office, Sandia National Laboratories, Los Alamos National Laboratory, the American Association of Port Authorities, and the George J. Kostas Research Institute for Homeland Security.

BACKGROUND

The U.S. maritime border includes 95,000 miles of open shoreline, 361 ports and an Exclusive Economic Zone that spans 3.5 million square 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 data shows 7,836 commercial vessels made 68,036 port calls in 2011. According to U.S. Customs and Border Protection (CBP), in 2014, 11 million shipping containers arrived on ships and entered U.S. seaports, representing nearly half of incoming U.S. trade (by value).

Standard sizes of shipping containers allow cargo to be quickly transferred from ships to trucks or railcars and transported efficiently to anywhere in the country. This rapid transfer of cargo has been viewed as a possible conduit and target for terrorist activities. The Department of Homeland Security (DHS) reported in 2009 that the likelihood of a terrorist smuggling weapons of mass destruction into the U.S. in shipping containers is low, the Nation's vulnerability to this

activity and consequences of such an attack – revenue losses, loss of lives, and disruption in manufacturing and other economic activities – are potentially high.

A "dirty bomb" is a type of radiological dispersal device (RDD) that combines conventional explosives, such as dynamite, with radioactive material. According to the U.S. Nuclear Regulatory Commission, an RDD would not release enough radiation to kill people or cause severe illness. The explosion from the conventional explosives used in the bomb would be more harmful to anyone near the event than the radioactive material. However, it is acknowledged that the use of an RDD is likely to create fear and panic, contaminate property, require a potentially costly cleanup, and if it occurred at a U.S. port, a shutdown of that port.

Radioisotopes, such as cobalt-60 and cesium-137, which can be used to construct an RDD, are fairly common radioactive elements with each having legitimate medical, commercial and industrial uses. Organizations such as the International Atomic Energy Agency warn that such radioisotopes are readily available to virtually any country in the world; moreover they are almost certainly not beyond the reach of even moderately capable non-state actors.

On October 7, 2015, the Associated Press reported that the Federal Bureau of Investigations (FBI), working with Eastern European authorities, over the last five years interrupted four attempts by criminal gangs with suspected Russian connections to sell radioactive material (cesium) to Middle Eastern extremists. The most recent attempt was in February 2015, in the Eastern European country of Moldova, where the sale was interrupted by authorities. This successful disruption showed that intelligence efforts to monitor movement of unregulated radioactive materials are working. Authorities stress the need to maintain these monitoring initiatives to deter or thwart this illegal trade in the future.

Prior to September 11, 2001, the primary focus of intermodal transportation was the safe movement of shipping containers in a timely manner. As a result of ongoing terrorist threats, the U.S. continues to develop and improve its security regime to minimize the risks and consequences of a terrorist attack without slowing the movement of cargo.

<u>Legislation enacted after 9/11 includes</u>:

- The Trade Act of 2002 (P.L. 107-210) requires importers and exporters to submit cargo manifest data 24 hours in advance of cargo arriving at a U.S. port.

- The Maritime Transportation and Security Act of 2002 (MTSA) (P.L. 107-295), now Chapter 701of title 46, Port Security, established DHS's overall role in the port security regime. It required DHS to review vessel and port security and develop regional and national maritime transportation security plans. It also created the Transportation Worker Identity Credential (TWIC) cards administered by the Transportation Security Administration (TSA) and the U.S. Coast Guard (Coast Guard). MTSA requires DHS to assess foreign port security measures and if a foreign port fails to maintain certain security standards, DHS can prohibit vessels coming from those foreign ports access to U.S. ports.

- The Security and Accountability for Every (SAFE) Port Act of 2006 (P.L. 1090-347) (6 U.S.C. 901 et. seq.) made adjustments to the MTSA and codified authorities for the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, and the Domestic Nuclear Detection Office.

- The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) (P.L. 110-53) amended the SAFE Port Act to require by July 2012, 100 percent of all U.S. bound shipping containers be scanned at foreign ports with both radiation-detection and nonintrusive inspection equipment before being placed on U.S.-bound vessels. The law allowed DHS to grant extensions to ports that cannot support 100 percent scanning.

Efforts to secure the supply chain

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 by different organizations based on their jurisdiction.

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.

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 (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 transitioned in 2005 from its Port Security Risk Assessment Tool (PS-RAT) to Maritime Security Risk Assessment Model (MSRAM). PS-RAT had allowed ports to prioritize resource allocation within a port, but not between ports. MSRAM allows port risk assessments across multiple ports, where USCG units assess risks-threats, vulnerabilities, and consequences-of a terrorist attack using different scenarios and targets and then applies MSRAM information to direct the allocation of USCG resources as needed to U.S. ports.

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.

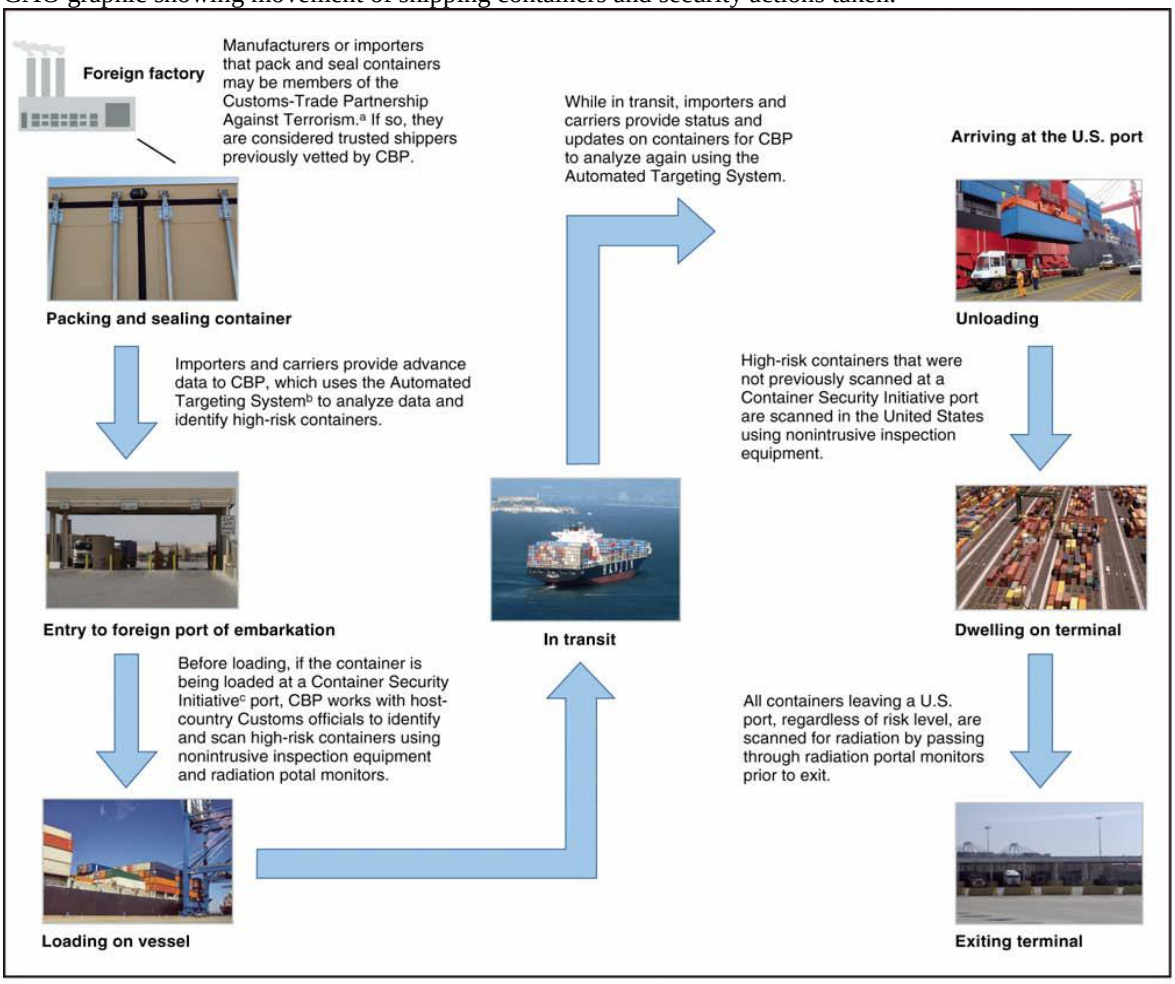
Per the Trade Act of 2002 (P.L. 107-210), cargo container manifests are required to be submitted to CBP 24 hours before shipping containers are loaded at a foreign port onto a U.S.-bound vessel. Other information collected by CBP, per the SAFE Port Act, is commonly referred to as "10+2" shipper information. This information includes ten 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 conducts 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 the 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. which 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.

GAO graphic showing movement of shipping containers and security actions taken:



Source: GAO (analysis); GAO and DHS S&T (photos) and Art Explosion (clipart).

The World Customs Organization (WCO) is the only international body dedicated exclusively to international customs and border control matters. CBP is the lead U.S. agency engaged with the WCO. CBP works with the WCO to integrate domestic measures including "10+2" data elements into international security standards.

If an NTC-C review of shipping container manifest data indicates a high-risk container, CBP will work with staff at CSI ports to get the high risk container scanned. Primary scanning is accomplished through the use of non-intrusive inspections (NII) which involve 1) large-scale X-ray and gamma ray imaging systems, and 2) Radiation Portal Monitor (RPM) for radiation. If the NII measures cannot resolve the issue, a physical inspection of the container will then occur. NTC-C staff also reviews manifest data for containers starting from non-CSI ports. NTC-C staff

will coordinate with U.S. State Department and local port authorities to get non-intrusive scanning or physical inspections for any identified high-risk containers.

CBP uses non-intrusive technology for cargo entering and leaving U.S. ports. Radiation Portal Monitors (RPMs), installed by the DHS, 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 some of the following materials plutonium, kitty litter and granite.

CBP’s 2014 Performance and Accountability Report notes that by the end of FY 2014, CBP deployed NII technologies to air, land, and sea ports of entry and to Border Patrol checkpoints including 314 large-scale imaging systems, 1,362 radiation portal monitors, 2,979 radiation isotope identification devices, and 30,305 personal radiation detectors. In 2014, CBP used these large-scale systems in more than 7.2 million examinations, resulting in more than 2,093 seizures and the interception of more than 249,200 pounds of narcotics. CBP says the technology provides a non-intrusive means to scan 100 percent of vehicles and shipping containers for radiation entering the country while facilitating the flow of legitimate travel and trade. CBP also states that 99 percent of all incoming containerized cargo arriving in the U.S. by sea is processed through an RPM.

In addition, the Border Security Deployment Program has an integrated surveillance and intrusion - detection system consisting of more than 8,400 cameras and microphones—that provide security, motion detection, and remote monitoring capabilities across every U.S. land port of entry. The system connects via the DHS Wide Area Network to remote monitoring stations called Customs Area Security Centers. These centralized command centers house digital video recorders augmented with analytic software to alert watch officers of a detected alarm or intrusion within a port facility and archive the event as evidence in subsequent investigations and prosecutions.

The SAFE Port Act (6 U.S.C. 981) required DHS to implement a Secure Freight Initiative (SFI) using non-intrusive imaging equipment and radiation detection equipment to scan shipping containers. DHS implemented the pilot project in 2007 at three international ports – Qasim in Pakistan, Puerto Cortes in Honduras, and Southhampton in United Kingdom. It was extended on a limited basis to the ports of Salalah in Oman, Busan in South Korea, and in Singapore. SFI was scaled back due to a number of issues, including lack of host state support and costs. CBP reported the cost of SFI pilot project was about $120 million over the first three years. In 2015, only the Port of Qasim in Pakistan is still operational.

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.

The SAFE Port Act (6 U.S.C. 982), as amended by the 9/11 Commission Act, also authorized the DHS Secretary to issue two-year extensions for foreign ports that could not meet the 100 percent scanning requirement. In May 2012, then-DHS Secretary Janet Napolitano issued a blanket two-year extension for all foreign ports; DHS Secretary Jeh Johnson subsequently issued another two-year extension in May 2014. Secretary Johnson noted in his letter to Congress regarding the extension, that DHS's ability to fully comply with 100 percent scanning is highly improbable. The Congressional Research Service March 20, 2015, report entitled *Transportation Security: Issues for the 114th Congress* mentions that U.S. trading partners do not support 100 percent scanning. It also noted a European Commission (EC) determination that 100 percent scanning is the wrong approach and that the EC supports a multilayered risk management approach.

Efforts to deter, detect, and respond to smuggling activities

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). DNDO implements the GNDA domestic component to detect and interdict nuclear smuggling. 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, that 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 technologies and protocols to address those gaps. End users of the technologies developed include CBP, USCG, Transportation Security Administration, state, local, and tribal law enforcement agencies.

DNDO is made up of seven Directorates. These directorates focus on the following activities:

- determining gaps or vulnerabilities in the GNDA
- conducting engineering development and deployment of technologies
- coordinating long-term research and development
- developing information sharing and analytical tools
- ensuring that DNDO proposes sound technical solutions and understands system performance and vulnerabilities

- providing national-level stewardship procedures, protocols, centralized planning and integration for nuclear forensics.

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.

GAO, in its March 2015 report entitled *Combating Nuclear Smuggling – DHS Research and Development on Radiation Detection Technology Could Be Strengthened* reviewed DNDO research programs and their ability to meet GNDA needs. GAO's performance audit ran from November 2013 to March 2015. GAO found that DNDO's TAR Directorate did not have documentation showing how its research and developed technologies resolve identified gaps in the GNDA. GAO recommended DNDO's TAR Directorate develop a research road map and implementation strategy to guide research. TAR should also better document how it prioritizes research, and it should develop a way to evaluate how research and development projects meet the TAR Directorate's overall research challenges (i.e. address gaps in the GNDA).

The September 2014 GAO (unclassified) report entitled *Combating Nuclear Smuggling – Risk-Informed Covert Assessment and Oversight of Corrective Actions Could Strengthen Capabilities at the Border* found that over the period of 2006 through 2013 CBP's Operational Field Testing Division (OFTD) conducted 144 covert operations at 86 locations out of 665 U.S. air, land, and sea port facilities; checkpoints; and certain international locations. These OFTD covert operations allow CBP to assess capabilities and procedures to detect and interdict or intercept nuclear and radiological materials at the 86 locations. GAO noted that while OFTD issues reports (although, not on a timely basis) that include recommendations for corrective actions, CBP does not track corrective actions taken to address areas of concern. GAO recommended creating a tracking mechanism to account for corrective measures taken at ports of entry and check points to assist in directing where resource investments (equipment and personnel training) should be made to assist CBP in deterring smuggling efforts.

A covert operation was considered successful, if a CBP officer or U.S. Border Protection agent both detected and interdicted the test source using standard operating procedures. GAO redacted the results of the 38 tests for security purposes. GAO noted in the report that CBP has not conducted risk assessments that could be incorporated into the decision making process for prioritizing materials, locations, and technologies tested in the covert operations and references a DHS 2010 Policy for Integrated Risk Management that says its components should use such assessments. CBP's 2013 Integrated Planning Guidance for fiscal years 2015 through 2019 included recommendations for integrating risk assessments into decision making, but CBP has not yet taken this step. GAO recommended in its report that the Secretary of Homeland Security conduct or use a risk assessment to inform department priorities and to assist CBP in getting information necessary for oversight and accountability – determine timeframes for OFTD reporting, and develop mechanisms to track corrective actions.

Maritime Domain Awareness

The 2013 *National Maritime Domain Awareness Plan for The National Strategy for Maritime Security* (2013 Plan) defines "Maritime Domain" as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people cargo, vessels and other conveyances. "Maritime Domain Awareness" is defined in the 2013 Plan as the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the U.S.

The FBI, DHS and DOD share responsibility to keep threats from entering the U.S.; however, should an event occur inside the U.S., the USCG and DHS support the FBI's lead for law enforcement. The Maritime Operational Threat Response (MOTR) facilitates interagency coordination for situations requiring multiple agencies coordination. The final MOTR plan was signed in 2006 and is the presidentially approved plan to achieve a coordinated U.S. government response to threats in the maritime domain. The Global MOTR Coordination Center was established in 2010 and includes the Departments of State, Defense, Justice, Commerce, Transportation, and Homeland Security.

Federal law authorizes the USCG to board any vessel subject to the jurisdiction, or operation of any law, of the U.S. in order to make inquiries, examinations, inspections, searches, seizures, and arrests for the violations of U.S. laws. The USCG may order and force any vessel to stop and may engage in land, water, and air patrols. Federal law also authorizes the USCG to control the anchorage and movement of vessels in the navigable waters of the U.S. Each USCG Captain of the Port may employ any additional security measures that he deems necessary to ensure the safety and security of the port, including prohibiting a vessel from entering the port. Per DHS, all USCG vessel boarding and inspection teams are equipped with nuclear/radiological detectors, with more than 72,000 boardings and 15,000 facility inspections conducted each year.

USCG uses the IMO sanctioned Automatic Identification System (AIS), which is the global standard for ship-to-ship, ship-to-shore, and shore-to-ship communications, as the basis for its Nationwide Automatic Identification System (NAIS). NAIS was initiated in response to the MTSA to enhance domain awareness with a focus on improved security, navigational safety, search and rescue, and environmental protection services.

All information collected by the USCG and CBP which is provided to NTC-C allows CBP and USCG to track where vessels, shipping containers, and crew have been and their locations prior to entering the U.S. In addition to tracking these cargo vessels, USCG and other law enforcement agencies face the challenge of distinguishing between legitimate small vessel operators and those involved in illicit activities. DHS's April 2008 Small Vessel Security Strategy (DHS 2008 Strategy) characterizes small vessels as any watercraft regardless of method of propulsion, less than 300 gross tons. Vessels less than 300 gross tons can 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. USCG statistics indicate there are approximately 17 million small vessels operating in U.S. waterways.

The goal of the DHS 2008 Strategy is to reduce potential security and safety risks from small vessels through adoption and implementation of a coherent system of regimes, awareness, and security operations by striking a balance between fundamental freedoms, adequate security, and continued economic stability. The DHS 2008 Strategy identified concerning scenarios which included a waterborne improvised explosive device. DHS and the USCG have strategies and programs in place to reduce small vessel risks, but the 2010 GAO report found there were still areas of concern including: loss of funding to support community outreach efforts; the lack of small vessel tracking systems; and funding constraints limiting security activities. The 2010 GAO report noted concerns stated in 2006 by then-Vice Admiral Thad Allen, Chief of Staff for the USCG, regarding concerns about small vessels posing a greater threat than containers for nuclear smuggling in testimony before the Senate Committee on Appropriations Subcommittee on Homeland Security.

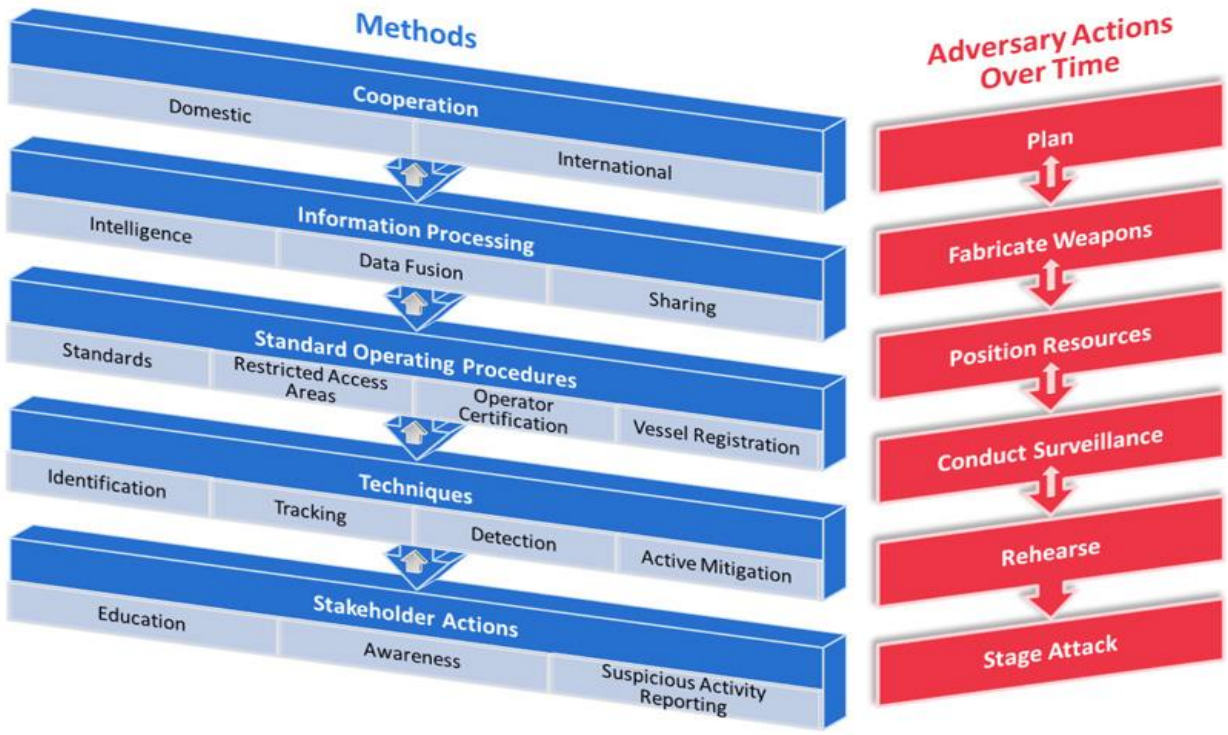
DNDO has tested boat-mounted radiation detectors, backpack carried detection equipment, and handheld radiological detection and identification devices. The January 2009 GAO report, "*Nuclear Detection – Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities"*, noted that DNDO tests revealed issues with the technology. Boat-mounted radiation equipment could not indicate the direction of the radioactive material causing the alarm. Backpack equipment works best when worn but it impeded USCG personnel when maneuvering on boats. Lastly, hand-held devices were expensive ($15,000 per unit) and did not float and did not withstand being submerged. The 2009 GAO report recommended DNDO take steps to work with the Departments of Defense, Energy, and State to develop an overarching strategic plan to guide efforts to combat nuclear smuggling. It also suggested that for DNDO's future efforts to combat nuclear smuggling on small vessels, DHS must develop criteria to assess the effectiveness, cost and feasibility of its pilot programs.

In 2011, DHS developed a Small Vessel Security Implementation Plan (Small Vessel Plan) after a multi-year process involving public and private stakeholders, DHS, and other federal, state, local and tribal authorities. The Small Vessel Plan is roadmap to realize the goals and objectives of the DHS 2008 Strategy. The Small Vessel Plan identifies possible and proven means of managing and controlling risks posed by the potential threat and possible dire consequences of small vessel exploitation by terrorists. The Small Vessel Plan been designated Security Sensitive Information due to its sensitive nature.

DHS released a report entitled *Small Vessel Security Implementation Plan Report to the Public* (Small Vessel Report). The Small Vessel Report notes the Small Vessel Plan employs a layered approach to achieve a defense in depth strategy against potential threats *(*see graphic on page 11).

DHS states that each layer of defense takes advantage of governmental authorities and capabilities, at times in coordination with stakeholder groups present, to disrupt adversary actions. While building on capabilities to act on information, the methods increase the potential of disrupting potential adversarial attacks and identify dangerous conditions and situations to allow for more effective responses to the broad array of situations that may be encountered in the maritime environment. These actions can improve readiness and responses to events and recovery from disasters. Federal partners, in conjunction with public and private stakeholders, build an informational system that facilitates and supports maritime homeland security.

DHS figure on the layered approach to achieve a defense in depth strategy:



WITNESSES

Panel I

Rear Admiral Peter J. Brown
Assistant Commandant for Response Policy
United States Coast Guard

Dr. Huban Gowadia
Director
Domestic Nuclear Detection Office

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

Mr. David C. Maurer
Director
Justice and Law Enforcement Issues
Homeland Security and Justice Team
U.S. Government Accountability Office

Panel II

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

Mr. Charles A. (Gus) Potter
Distinguished Member of the Technical Staff
Sandia National Laboratories

Mr. Joe Lawless
Chairman
Security Committee
American Association of Port Authorities

Mr. Stephen Flynn, Ph.D.
Director
Center for Resilience Studies
Northeastern University