

# AN EXAMINATION OF THE MARITIME NUCLEAR SMUGGLING THREAT AND OTHER PORT SEC- URITY AND SMUGGLING RISKS IN THE UNITED STATES

---

Committee on Transportation and Infrastructure  
Serial No. 114-48  
Committee on Homeland Security  
Serial No. 114-79

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COAST GUARD AND MARITIME  
TRANSPORTATION,

COMMITTEE ON TRANSPORTATION AND  
INFRASTRUCTURE

AND THE

SUBCOMMITTEE ON BORDER AND MARITIME  
SECURITY,

COMMITTEE ON HOMELAND SECURITY  
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

---

JULY 7, 2016

---

Printed for the use of the Committee on Transportation and Infrastructure and  
the Committee on Homeland Security



Available online at: [http://www.gpo.gov/fdsys/browse/  
committee.action?chamber=house&committee=transportation](http://www.gpo.gov/fdsys/browse/committee.action?chamber=house&committee=transportation)

U.S. GOVERNMENT PUBLISHING OFFICE

20-639 PDF

WASHINGTON : 2016

---

For sale by the Superintendent of Documents, U.S. Government Publishing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

## COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

BILL SHUSTER, Pennsylvania, *Chairman*

DON YOUNG, Alaska	PETER A. DeFAZIO, Oregon
JOHN J. DUNCAN, JR., Tennessee, <i>Vice Chair</i>	ELEANOR HOLMES NORTON, District of Columbia
JOHN L. MICA, Florida	JERROLD NADLER, New York
FRANK A. LOBIONDO, New Jersey	CORRINE BROWN, Florida
SAM GRAVES, Missouri	EDDIE BERNICE JOHNSON, Texas
CANDICE S. MILLER, Michigan	ELIJAH E. CUMMINGS, Maryland
DUNCAN HUNTER, California	RICK LARSEN, Washington
ERIC A. "RICK" CRAWFORD, Arkansas	MICHAEL E. CAPUANO, Massachusetts
LOU BARLETTA, Pennsylvania	GRACE F. NAPOLITANO, California
BLAKE FARENTHOLD, Texas	DANIEL LIPINSKI, Illinois
BOB GIBBS, Ohio	STEVE COHEN, Tennessee
RICHARD L. HANNA, New York	ALBIO SIRES, New Jersey
DANIEL WEBSTER, Florida	DONNA F. EDWARDS, Maryland
JEFF DENHAM, California	JOHN GARAMENDI, California
REID J. RIBBLE, Wisconsin	ANDRÉ CARSON, Indiana
THOMAS MASSIE, Kentucky	JANICE HAHN, California
MARK MEADOWS, North Carolina	RICHARD M. NOLAN, Minnesota
SCOTT PERRY, Pennsylvania	ANN KIRKPATRICK, Arizona
RODNEY DAVIS, Illinois	DINA TITUS, Nevada
MARK SANFORD, South Carolina	SEAN PATRICK MALONEY, New York
ROB WOODALL, Georgia	ELIZABETH H. ESTY, Connecticut
TODD ROKITA, Indiana	LOIS FRANKEL, Florida
JOHN KATKO, New York	CHERI BUSTOS, Illinois
BRIAN BABIN, Texas	JARED HUFFMAN, California
CRESENT HARDY, Nevada	JULIA BROWNLEY, California
RYAN A. COSTELLO, Pennsylvania	
GARRET GRAVES, Louisiana	
MIMI WALTERS, California	
BARBARA COMSTOCK, Virginia	
CARLOS CURBELO, Florida	
DAVID ROUZER, North Carolina	
LEE M. ZELDIN, New York	
MIKE BOST, Illinois	

---

## SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

DUNCAN HUNTER, California, *Chairman*

DON YOUNG, Alaska	JOHN GARAMENDI, California
FRANK A. LOBIONDO, New Jersey	ELIJAH E. CUMMINGS, Maryland
BOB GIBBS, Ohio	CORRINE BROWN, Florida
MARK SANFORD, South Carolina	JANICE HAHN, California
GARRET GRAVES, Louisiana	LOIS FRANKEL, Florida
CARLOS CURBELO, Florida	JULIA BROWNLEY, California
DAVID ROUZER, North Carolina	PETER A. DeFAZIO, Oregon ( <i>Ex Officio</i> )
LEE M. ZELDIN, New York	
BILL SHUSTER, Pennsylvania ( <i>Ex Officio</i> )	

## COMMITTEE ON HOMELAND SECURITY

MICHAEL T. McCAUL, Texas, *Chairman*

LAMAR SMITH, Texas	BENNIE G. THOMPSON, Mississippi
PETER T. KING, New York	LORETTA SANCHEZ, California
MIKE ROGERS, Alabama	SHEILA JACKSON LEE, Texas
CANDICE S. MILLER, Michigan, <i>Vice Chair</i>	JAMES R. LANGEVIN, Rhode Island
JEFF DUNCAN, South Carolina	BRIAN HIGGINS, New York
TOM MARINO, Pennsylvania	CEDRIC L. RICHMOND, Louisiana
LOU BARLETTA, Pennsylvania	WILLIAM R. KEATING, Massachusetts
SCOTT PERRY, Pennsylvania	DONALD M. PAYNE, JR., New Jersey
CURT CLAWSON, Florida	FILEMON VELA, Texas
JOHN KATKO, New York	BONNIE WATSON COLEMAN, New Jersey
WILL HURD, Texas	KATHLEEN M. RICE, New York
EARL L. "BUDDY" CARTER, Georgia	NORMA J. TORRES, California
MARK WALKER, North Carolina	
BARRY LOUDERMILK, Georgia	
MARTHA MCSALLY, Arizona	
JOHN RATCLIFFE, Texas	
DANIEL M. DONOVAN, Jr., New York	

BRENDAN P. SHIELDS, *Staff Director*  
JOAN V. O'HARA, *General Counsel*  
MICHAEL S. TWINCHEK, *Chief Clerk*  
I. LANIER AVANT, *Minority Staff Director*

---

## SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

MARTHA MCSALLY, Arizona, *Chairman*

LAMAR SMITH, Texas	FILEMON VELA, Texas
MIKE ROGERS, Alabama	LORETTA SANCHEZ, California
CANDICE S. MILLER, Michigan	SHEILA JACKSON LEE, Texas
JEFF DUNCAN, South Carolina	BRIAN HIGGINS, New York
LOU BARLETTA, Pennsylvania	NORMA J. TORRES, California
WILL HURD, Texas	BENNIE G. THOMPSON, Mississippi ( <i>Ex</i>
MICHAEL T. McCAUL, Texas ( <i>Ex Officio</i> )	<i>Officio</i> )

PAUL L. ANSTINE, *Subcommittee Staff Director*  
JOHN DICKHAUS, *Subcommittee Clerk*  
ALISON NORTHROP, *Minority Subcommittee Staff Director*



## CONTENTS

	Page
Summary of Subject Matter from the Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure .....	vi
TESTIMONY	
PANEL 1	
Rear Admiral Linda L. Fagan, Deputy Commandant for Operations, Policy, and Capabilities, U.S. Coast Guard .....	4
L. Wayne Brasure, Ph.D., Acting Director, Domestic Nuclear Detection Office .....	4
Todd C. Owen, Executive Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection .....	4
Anne Harrington, Deputy Administrator for Defense Nuclear Nonproliferation, National Nuclear Security Administration .....	4
PANEL 2	
Jennifer A. Grover, Director, Homeland Security and Justice, U.S. Government Accountability Office .....	24
Gregory H. Canavan, Ph.D., Senior Fellow, Los Alamos National Laboratories .....	24
David A. Espie, Director of Security, Maryland Port Administration, Port of Baltimore, on behalf of the American Association of Port Authorities .....	24
James H.I. Weakley, President, Lake Carriers' Association .....	24
PREPARED STATEMENTS SUBMITTED BY MEMBERS OF CONGRESS	
Hon. John Garamendi of California .....	45
PREPARED STATEMENTS SUBMITTED BY WITNESSES	
Rear Admiral Linda L. Fagan .....	49
L. Wayne Brasure, Ph.D. ....	53
Todd C. Owen .....	59
Anne Harrington .....	69
Jennifer A. Grover .....	78
Gregory H. Canavan, Ph.D. ....	96
David A. Espie .....	104
James H.I. Weakley .....	109
SUBMISSIONS FOR THE RECORD	
Rear Admiral Linda L. Fagan, Deputy Commandant for Operations, Policy, and Capabilities, U.S. Coast Guard, responses to requests for information from the following Representatives:	
Hon. Bob Gibbs of Ohio .....	17
Hon. Carlos Curbelo of Florida .....	22
Article entitled, "U.S. Ports Want More Action on Dirty Bomb Prevention," Maritime Executive, July 6, 2016, submitted by Hon. Sheila Jackson Lee of Texas .....	116
Letter of July 1, 2016, to Hon. Jeh Johnson, Secretary, Department of Homeland Security, from 47 Members of Congress, submitted by witness David A. Espie .....	118



**Committee on Transportation and Infrastructure  
U.S. House of Representatives**

Washington, DC 20515

**Bill Shuster**  
Chairman

**Peter A. DeFazio**  
Ranking Member

Christopher P. Bertone, Staff Director

Katherine W. Hedrick, Legislative 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**

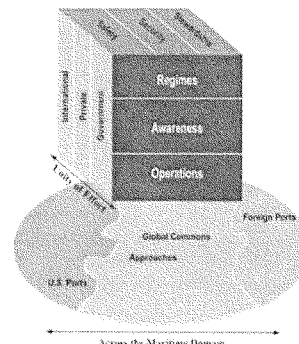
The global Maritime Transportation System (MTS) is an interconnected system of waterways, ports, terminals, intermodal connections, vessels, people, support service industries

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.

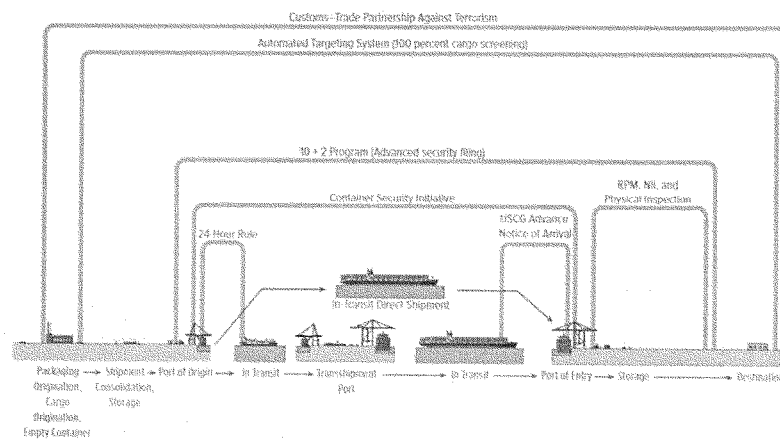
The DHS Small Vessel Security Implementation Plan (*Plan*) was developed as a roadmap for meeting the goals and objectives of the *Strategy* and is intended as a guidance document not a

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 high 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 benchmark 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

APPENDIX100 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.



# **AN EXAMINATION OF THE MARITIME NUCLEAR SMUGGLING THREAT AND OTHER PORT SECURITY AND SMUGGLING RISKS IN THE UNITED STATES**

**THURSDAY, JULY 7, 2016**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON COAST GUARD AND MARITIME  
TRANSPORTATION,  
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,  
JOINT WITH THE  
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY,  
COMMITTEE ON HOMELAND SECURITY,  
*Washington, DC.*

The subcommittees met, pursuant to notice, at 10:08 a.m. in room 2167, Rayburn House Office Building, Hon. Duncan Hunter (Chairman of the Subcommittee on Coast Guard and Maritime Transportation) presiding.

Mr. HUNTER. The subcommittee will come to order.

The subcommittee is meeting today to examine the efforts of the Department of Homeland Security to prevent the smuggling of nuclear materials in U.S. ports and other port security risks. This hearing follows last year's hearing which examined the prevention and response to a dirty bomb at a U.S. port. And we had a classified hearing yesterday. We are going to make sure and skirt around those topics which we talked about yesterday and we are not going to talk about today in an open hearing.

It seems clear that Islamic extremists aspire to carry out a radiological or nuclear attack, so this is a threat that we obviously need to take seriously. If anybody succeeds even once, the consequences would be catastrophic. To be prepared, we must ensure that we have the proper screening and response protocols in place.

Today we will continue to review these efforts as well as the broader governmental efforts to reduce threats to our ports and our borders. I want to thank Chairwoman Martha McSally, who will be here momentarily, and the House Committee on Homeland Security for agreeing to explore this important topic in a joint hearing.

The security of our maritime ports and borders remains a serious concern for the United States. Our Nation relies on the commerce that flows through our ports including the more than 41 percent of foreign trade that is moved on vessels every year. Providing adequate security requires an innovative, multifaceted approach which has to begin far from U.S. shores and has to be flexible enough to keep pace with the ever-changing threats to our national security.

After 9/11, security measures were enacted to better protect our homeland by expanding efforts to detect and deter threats overseas. These efforts include screening cargo manifests before containers are loaded onto a U.S.-bound ship, scanning shipping containers that have been determined to be high-risk, screening ship personnel data, and tracking ships and their cargo as they make their way to our shores. Despite these efforts, we want to make sure that we are still employing the best technology to detect the presence of nuclear or radiological material in containerized cargo.

However, containers are not the only avenue for smuggling harmful materials and weapons into the U.S. ports. Small vessels pose an equally devastating threat and are just as difficult as containers to determine legitimate uses from potential threats. Commercial and recreational small vessels can easily blend into the daily activity of U.S. waterways and can be converted to stand-off weapons platforms, or used as direct attacks to deliver a waterborne IED [improvised explosive device].

We will hear from our witnesses today on how the Federal Government deploys a whole-of-government, layered approach including law enforcement, technology, and intelligence to detect, deter, and interdict potential threats. These internal measures are combined with treaties and agreements with foreign governments to conduct cooperative enforcement efforts overseas. That is one of the things that I found most interesting about what we are going to hear about today, is how far out we reach and the nations that work with us to make us safe back here at home.

I look forward to continuing our discussion from last year and learning more about the ongoing efforts to keep our ports and Nation safe.

With that, I yield to Chairwoman McSally.

Ms. MCSALLY. Thank you, Mr. Chairman. And thanks for our witnesses' comments today on this very important topic. We had a good discussion in the classified realm yesterday, and look forward to a good discussion today on this very serious threat.

We know that terrorist organizations, in my lifetime, in 26 years in the military, have been plotting and wanting to do the maximum amount of harm to our country and our way of life and our interests. The worst-case scenario that both my colleague and I, as we served in the military, was always a combination of terrorist organizations and weapons of mass destruction of various kinds. And in my role in homeland security we have addressed some of these other biological, chemical threats. Today I appreciate that we are highlighting the radiological and nuclear potential threats of that nexus between terrorist organizations getting access to these deadly weapons.

We learned in my time in the military that threat equals capability plus intent. We have seen, through open-source reporting, that they clearly have the intent, you know, to maximize harm against America, the West, and our way of life. Certainly they have declared that intent through whatever means possible, and the devastation that would come from having such a capability in an attack would be severe, as we know, not just for the death and the loss of life and the impact on the economy, but also the fear that



it would invoke, which is, you know, certainly a motivation of the terrorists.

So, as we look at now the capability—and I know we are in an unclassified realm—I look forward to hearing from our experts today about what the threat is. Now, we don't want to be tipping our hand or highlighting to the enemy any of our vulnerabilities, so we need to be very careful as we are highlighting what these threats are, so that we can make sure that we are doing everything we can through a whole-of-society, whole-of-government, with our partners, in order to address and mitigate and detect and interdict these threats.

We need to make sure that we highlight this in hearings like today so that we are doing all that we can to make sure that we are stopping any sort of attack from a radiological or a nuclear weapon from a terrorist organization like ISIS [Islamic State of Iraq and Syria].

There are many pathways that these individuals could use in order to bring a weapon like this into our country. I live in a southern border district. That is certainly one pathway. Coming in through air, coming in through maritime, through our seaports of entry, small boats, all these types of things are ones that—we have seen the drug supply come through. And so I am interested to, you know, hear from our witnesses specifically about the threat. And again, to the maximum extent possible in the unclassified realm, you know, what we are doing about it and what more we could do about it.

We do know that there has been just, again, recent reports revealing radiological nuclear material being lost or stolen several times a year, especially in Russia and other former Soviet States. Just as an example, several years ago FBI [Federal Bureau of Investigation] was involved in a sting operation that disrupted the sale of cesium which would have been enough to contaminate several city blocks. So this is the type of threat.

The weapons-grade nuclear capability and the radiological threat that we are very interested in investigating further today, we appreciate the expertise and the service of our witnesses. And I yield back.

Mr. HUNTER. I thank the gentlelady. Mr. Garamendi is recognized. You are all lucky. You get four opening statements instead of two today. You're welcome.

Mr. GARAMENDI. Reviewing my statement earlier today and realizing there are four opening statements, Mr. Chairman, I would ask unanimous consent that my statement be in the record, and I will simply summarize very, very quickly, so that we can get on with hearing from the witnesses.

We have got about 95,000 miles of coastal area in the United States. We have got 360 ports of various sizes around the Nation, and islands, and so forth, all of which present an opportunity for bad things to happen. We are going to talk about those nuclear issues, the biological issues, all of those, and I look forward to hearing from the witnesses.

A very complex issue in many, many ways, but one that we have to deal with. Dirty bombs, real bombs, biological issues, and quite possibly we are now learning with Zika and yellow fever that it

may just be a human that is infected coming in from an African port or a South American port that could initiate a major public health crisis in the United States.

And so these threats are real, they have to be addressed. The witnesses are well versed in these issues, and I am looking forward to hearing from them. And with that I yield back.

Mr. HUNTER. I thank the ranking member. Mr. Vela is recognized.

Mr. VELA. I would essentially adopt the comments of my colleagues and, for the sake of time, I would just say that I represent about 200 miles of the Gulf of Mexico along the—right along the U.S.-Mexico border in south Texas. But for the sake of time I would also yield back.

Mr. HUNTER. All right. We begin our first panel today with Rear Admiral Linda Fagan, the Coast Guard's Deputy Commandant for Operations, Policy, and Capabilities.

Rear Admiral Fagan, you are recognized to make your statement.

**TESTIMONY OF REAR ADMIRAL LINDA L. FAGAN, DEPUTY COMMANDANT FOR OPERATIONS, POLICY, AND CAPABILITIES, U.S. COAST GUARD; L. WAYNE BRASURE, PH.D., ACTING DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE; TODD C. OWEN, EXECUTIVE ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION; AND ANNE HARRINGTON, DEPUTY ADMINISTRATOR FOR DEFENSE NUCLEAR NONPROLIFERATION, NATIONAL NUCLEAR SECURITY ADMINISTRATION**

Admiral FAGAN. Good morning, Chairman Hunter, thank you. Chairman McSally, Ranking Member Garamendi, Ranking Member Vela, and distinguished members of the subcommittees, it is my pleasure to be here today to discuss the Coast Guard's efforts in preventing smuggling in U.S. ports. I thank you for your strong support of the Coast Guard and our men and women in uniform. It is a pleasure to be here alongside my Department of Homeland Security colleagues, Assistant Commissioner Owen, Director Brasure, as well as our Department of Energy partner, Deputy Administrator Harrington.

My complete statement has been provided to the subcommittee and I ask that it be entered into the record.

By leveraging our expansive legal authorities, offshore maritime presence, and utilizing a layered approach to maritime border security, the Coast Guard pushes maritime border security and enforcement out well beyond the Nation's shoreline and exclusive economic zones. As a member of the intelligence community, and through strategic relationships with our interagency and international partners, we detect, deter, and counter threats as early and as far from the U.S. shores as possible.

The persistent threats that we face include illegal migration, human trafficking, illicit flow of drugs, and smuggling of weapons of mass destruction. My testimony today will focus on the layered Coast Guard efforts to prevent smuggling of nuclear devices into U.S. ports. However, many of the initiatives, programs, and capabilities I will highlight enable the Coast Guard to prevent and respond to a multitude of threats we face.

The Coast Guard's efforts to prevent smuggling of nuclear devices into U.S. ports and shores begins overseas. By leveraging international partnerships, as well as the International Port Security Program, the Coast Guard performs in-country port security assessments to determine the effectiveness of security and antiterrorism measures of our foreign training partners.

Since the program's inception in 2004, we have visited 150 countries and evaluated 1,200 port facilities. The Coast Guard maintains more than 40 maritime bilateral law enforcement agreements and 11 bilateral proliferation security initiative ship-boarding engagements. These agreements facilitate international cooperation and allow Coast Guard teams to board and search vessels at sea suspected of carrying illicit shipments of weapons of mass destruction, their delivery systems, or related materials.

The Coast Guard's membership within the intelligence community provides global situation awareness, analysis, interagency collaboration, opportunities with various counterterrorism components, including the Central Intelligence Agency, National Counterterrorism Center, and the Federal Bureau of Investigation. Direct, timely intelligence is a key enabler across a broad spectrum of threats.

Cargo crosses the ocean and nears our shores. Coast Guard personnel located with the Customs and Border Protection National Targeting Center screens ship, crew, and passenger information. In 2015 there were over 121,000 notice-of-arrivals and 32 million crew and passenger records screened by this team.

As ships arrive in American waters, our authorities through the Maritime Transportation Security Act provide a robust regime of security plan approval and compliance inspections for both maritime facilities and vessels.

Area Maritime Security Committees provide a recurring forum for key agencies and partners to address risks at each port. Through these committees we have training programs that focus on preventing and responding to transportation security incidents, and these are regularly exercised in the ports. And, for example, since 2003 the Coast Guard has partaken or participated in over two dozen dirty bomb scenarios through this exercise program.

Focusing specifically on the nuclear threat, in 2004 the Coast Guard developed and implemented a Servicewide Maritime Radiation Detection Program, partnering with the Domestic Nuclear Detection Office. We use their standards in all of our ships, and boarding officers are equipped with detection devices.

Providing significant and unique maritime response capabilities, the Coast Guard's Maritime Security Response Teams are able to detect and identify nuclear and radiological material and protect personnel in both routine and hostile situations. Should the country face a—knowledge of a radiological or nuclear device being suspected of smuggling, we would use the interagency maritime operational threat response protocols to bring in interagency coordination together to ensure an appropriate Government response.

The Coast Guard's response to a nuclear detonation in the maritime domain would be part of a larger interagency effort to bring the most appropriate national resources and capabilities to bear. We focus on the safety of American lives and the swift restoration

of commerce. Our unique maritime authorities, jurisdiction, and capabilities ensure the Coast Guard can provide security, command-and-control, transportation, and support to other agencies that need to operate in the maritime today.

For over two centuries the U.S. Coast Guard has safeguarded our Nation's maritime interests. A nuclear threat response scenario would require a whole-of-government coordinated interagency effort. The Coast Guard's layered security strategy, day-to-day operations, and coordination across the Government ensure that we are well-positioned to address the broad range of offshore and coastal threats.

I have only touched on a few of these layers in my opening comments, and I look forward to discussing these and other vital work the men and women of the Coast Guard do every day during your questions.

Thank you for the opportunity to appear before you today, and thank you for your continued support of the United States Coast Guard. Thank you.

Mr. HUNTER. Thanks, Admiral. Our next witness is Dr. Wayne Brasure, the Acting Director of the Domestic Nuclear Detection Office.

Dr. Brasure, you are recognized.

Dr. BRASURE. Good morning, Chairman Hunter, Chairwoman McSally, Ranking Member Garamendi, Ranking Member Vela, and distinguished members of the subcommittees. Thank you for the opportunity to be here with my colleagues from the Department of Homeland Security and the Department of Energy to discuss efforts to prevent smuggling at U.S. ports.

An attack on U.S. territory with a nuclear device or radiological dispersal device would have grave consequences. At the Domestic Nuclear Detection Office, or DNDO, we have a singular focus: preventing nuclear terrorism. It cannot be accomplished by any one agency. In fact, it takes a whole-of-enterprise approach. We work closely with our Federal, State, local, tribal, territorial, and international partners, as well as those in the national laboratories, industry and academia.

DNDO was established to develop, in coordination with the interagency, the Global Nuclear Detection Architecture, or the GNDA. The GNDA is a framework for detecting, analyzing, and reporting nuclear and other radioactive materials that are out of regulatory control.

In our work to enhance the GNDA we rely on a critical triad of intelligence, law enforcement, and technical capabilities. Our strategy is to provide effective technologies to well-trained law enforcement and public safety officials as they conduct intelligence-driven operations. Through a multilayered, multifaceted defense-in-depth approach, our objective is to make nuclear terrorism a prohibitively difficult undertaking for the adversary. We take into account the geographic layers of the GNDA, both international and domestic, as well as the pathways through which the material can be transited, such as the maritime and aviation pathways.

And so, our efforts to secure the homeland begin overseas, working closely with our interagency partners which have responsibility for implementing the international component of the GNDA. With

these partners and with multilateral organizations, the DNDO works to develop and share guidance, best practices, and training for the international community.

Ultimately, building a Global Nuclear Detection Architecture relies on sovereign foreign partners developing and enhancing their own national detection programs. The collective efforts abroad help ensure that illicit nuclear or other radioactive material or devices can be interdicted before they arrive at our shores.

As part of DNDO's responsibilities to implement the domestic component of the GNDA, we equip DHS [Department of Homeland Security] operational components with radiation detection systems for use at our ports of entry, along our land and maritime borders, and within the United States. In particular, DNDO equips both U.S. Coast Guard and U.S. Customs and Border Protection with radiation detection equipment.

Today all Coast Guard boarding parties are equipped with detection devices. At our seaports of entry, CBP [U.S. Customs and Border Protection] scans nearly 100 percent of all incoming containerized cargo for radiological and nuclear threats. DNDO has acquired systems for the Coast Guard and CBP to detect threats when encountering small vessels. We recently procured a new technology called Human Portable Tripwire to enable our partners to more quickly detect, identify, and adjudicate alarms relating to nuclear and other radioactive sources.

Building operational capability across the Federal, State, and local enterprise is also critical. DNDO is presently working with 36 of the Coast Guard's Area Maritime Security Committees. Through these committees we can share information and intelligence, assist with alarm adjudication, and provide technical support to our operational partners as they build their nuclear detection programs.

In the event of an interdiction of radioactive materials or an act of radiological or nuclear terrorism, the U.S. Government would need rampant accurate attribution based on sound scientific evidence. For this reason, we enhance the Nation's capabilities in technical nuclear forensics which, when coupled with intelligence and law enforcement information, support such determinations.

To bolster readiness of the U.S. Government's nuclear forensics capability in the maritime environment, we recently led the planning for and also participated in an exercise where an interagency task force coordinated the collection of simulated forensic evidence at sea.

Advancing the operational readiness of partners will ensure that leadership has the evidence so they can hold fully accountable any State, terrorist group, or other nonstate actor that supports or enables terrorist efforts to obtain or use weapons of mass destruction. An act of nuclear terrorism would have profound consequences for our Nation and the world. With your support, we will continue to work with our partners to bolster defenses to secure maritime ports and our homeland from nuclear terrorism.

Thank you for this opportunity, and I look forward to your questions.

Mr. HUNTER. Thank you, Doctor. Our next witness is Mr. Todd Owen, Executive Assistant Commissioner of the Office of Field Operations for U.S. Customs and Border Protection.

Mr. Owen, you are recognized.

Mr. OWEN. Thank you. Good morning, Chairman Hunter, Chairwoman McSally, Ranking Members Garamendi and Vela, and esteemed members of the subcommittees. Thank you for the opportunity to testify here today to discuss the role of U.S. Customs and Border Protection in the prevention and detection of smuggling activities at our ports of entry, an important responsibility we share with our partners here today.

As the lead DHS agency for border security, CBP works closely with our domestic and international partners to protect the Nation from a variety of dynamic threats, including those posed by containerized cargo arriving at our air, land, and sea ports. Before my appointment as the Executive Assistant Commissioner for the Office of Field Operations in February of 2015, I served in numerous capacities within CBP, most recently as the Director of Field Operations for the Greater Los Angeles area, including the L.A./Long Beach seaport. I have also served as the Executive Director over all of CBP's cargo security programs, and I know firsthand how complex cargo security operations are, and how valuable our programs and partnerships are to our national security.

Since the September 11 terrorist attacks, CBP has established security partnerships, enhanced our targeting and risk assessment programs, and invested in advance technology, all essential elements to our multilayer approach to protecting the Nation from the arrival of dangerous materials, including radiological and nuclear materials, at our ports of entry. CBP has several key programs that enhance our ability to assess cargo for risk, examine high-risk shipments at the earliest possible point, and increase the security of the supply chain. And I would like to highlight just a few of these efforts today.

First, CBP receives advanced information on every cargo shipment, every vessel, and every person before they arrive at our ports of entry.

Second, our advance targeting techniques use the advanced data to enhance our ability to assess risk associated with these cargo shipments and with the entities involved. The National Targeting Center, using the Automated Targeting System, has developed state-of-the-art capabilities to assess cargo shipments before they are laid and on board vessels destined for the United States.

Third, our partnerships, those with DHS and our other Federal partners, private industry, and foreign counterparts, increase information-sharing and enhance our domain awareness, our targeting capabilities, and the ability to intercept threats approaching our borders.

Pushing our security efforts outward, the Container Security Initiative, which was established specifically to prevent the use of maritime containerized cargo to transport a weapon of mass effect or destruction, enables CBP to work with foreign authorities to identify and examine potentially high-risk maritime containers at the first foreign ports, before they are laid and on board a vessel destined for the U.S. CBP now has 60 Container Security Initiative ports in 35 countries, and we screen over 80 percent of the maritime containerized cargo before it heads to the United States.

And finally, in partnership with DNDO, CBP has deployed nuclear and radiological detection equipment, including radiation portal monitors, radio isotope identification devices, and personal radiation detectors, nationwide. Using radiation portal monitors at our ports of entry, CBP is able to scan 100 percent of all mail and express consignment parcels, 100 percent of all truck cargo and personally owned vehicles arriving from Canada and Mexico, and 100 percent of all arriving maritime containerized cargo for the presence of radiological or nuclear materials.

CBP's detection technology, targeting capabilities, and partnerships are strategically aligned to prevent the arrival of dangerous materials or a dangerous weapon at a U.S. port. However, if such an event were to occur, CBP has established contingency plans and standard procedures to ensure a coordinated and effective response. In the event CBP detects a suspected radioactive source, all personnel are trained in secure, isolate, and notify protocols. The cargo is secured, the immediate area is isolated, and the scientific experts are notified. CBP scientists at the CBP Teleforensic Center in northern Virginia will confer with the Department of Energy, and, when necessary, refer the findings to the FBI to coordinate the appropriate response. All of these elements are part of a comprehensive cargo security strategy that enables CBP to identify and address the potential use of containerized cargo to transport radiologic weapons before they arrive at our Nation's ports of entry.

Thank you for the opportunity to testify today, and I will be happy to answer your questions.

Mr. HUNTER. Thanks, Mr. Owen. Our next witness is Ms. Anne Harrington, the Deputy Administrator for Defense Nuclear Non-proliferation at the National Nuclear Security Administration.

Ms. Harrington, you are recognized.

Ms. HARRINGTON. Thank you. Chairman Hunter, Chairwoman McSally, Ranking Members Garamendi and Vela, and distinguished members of the subcommittees, thank you for giving me the opportunity to discuss the Department of Energy's National Nuclear Security Administration's efforts to detect, deter, and investigate the illicit smuggling of nuclear and other radioactive materials. My full statement has been provided and I ask that it be entered into the record.

I am also very pleased to be appearing today with colleagues from the Department of Homeland Security. You should look at the four witnesses in front of you as a team, because that is, indeed, how we work.

Securing nuclear and radiological materials from theft, diversion, or trafficking is a critical element of U.S. national security strategy. Despite significant progress over the last 20 years by international cooperative programs, gaps remain and interest in acquiring these materials persist.

The threat landscape as we see it today includes over 30 countries with weapon-usable nuclear material stored at hundreds of sites, with the largest inventory in Russia; more than 100 countries with radiological material stored at thousands of sites, many of which lack adequate security; a demonstrated black market for nuclear and radiological materials, as shown by recent interdictions in Georgia and Moldova; and terrorist groups that have taken root

in ungoverned or undergoverned spaces, compounded by the emergence of Daesh or ISIL [Islamic State of Iraq and the Levant], a pseudostate with demonstrated capability to conduct international terrorist operations and an expressed interest in acquiring and using radiological and possibly nuclear materials against Western interests.

We take our job seriously because the consequences are so high. The use of a high-yield, improvised nuclear device, or IND, in a major U.S. city would cause hundreds of thousands of fatalities. The use of a radiological dispersal device, or RDD, would not cause the same loss of human life, but would be highly destabilizing, with broad physical, economic, and psychological consequences, demanding significant resources and a multifaceted response.

To counter this threat, the U.S. Government uses multiple means to prevent terrorists from obtaining nuclear and radiological materials. Within my organization, the Office of Defense Nuclear Non-proliferation, our Global Material Security program specializes in collaborating with partners worldwide to build sustainable capacity to secure nuclear weapons, weapons-usable materials, and radiological material, and to detect and investigate illicit trafficking of those materials.

We serve as the farthest exterior ring of protection for the United States. Our approach is simple: our first line of defense is to secure nuclear and radiological material at the source, and not allow it to be removed from regulatory control. Recognizing that this may not be enough, we have a second line of defense: our Nuclear Smuggling Detection and Deterrence program, or NSDD.

NSDD is a critical component of the Global Nuclear Detection Architecture. We deploy radiation detection systems internationally at official crossing points along rugged, unofficial borders in disputed territories which we call green borders, and along maritime borders, or blue borders, and at internal locations for law enforcement operations, working with our foreign partners, much the way the Department of Homeland Security works within the United States.

More importantly, our goal is to build the capacity, infrastructure, and relationships necessary to sustain these efforts into the future, and to cooperate with us in those efforts. The GNDA is predicated on a layered defense of law enforcement, intelligence, and technology to maximize a system of detection and deterrence capability. In the words of DHS's Domestic Nuclear Detection Office, NSDD is the largest single program in the exterior layer, and provides significant potential to stop a U.S.-bound terrorist attack outside our borders.

We have equipped 585 sites, including 46 large-container sea-ports, have provided 104 mobile radiation detection vans, and countless other handheld equipment. With this technology comes training, exercises, and sustainment support.

We also focus on sustainability, and have already transitioned 85 percent of our installations to full support by the host countries. We have taken important steps in countering the nuclear and radiological smuggling threat by developing a range of technologies, as already mentioned by our friends in DNDO, and we work closely together to establish the standards for those technologies.



NSDD's ability to adapt to an evolving threat, engage diverse international partnerships, and its ongoing collaboration with the interagency and with international organizations uniquely position this program to remain a leader in deploying and sustaining core elements of the Global Nuclear Detection Architecture, with the ultimate goal of preventing the use of a nuclear weapon or dirty bomb in the United States.

Thank you for your attention, and I will be happy to respond to your questions.

Mr. HUNTER. Thank you, Ms. Harrington. I am now going to recognize Members for questioning.

I guess the one thing that I am going to comment on is this. With terrorism and Islamic extremism where it is now, and the ability for nonstate actors to get ahold of nuclear weapons, or to get ahold of radiological weapons, or let's just say weapons of mass destruction of any kind, to have it nonattributable to any State, so there is no reciprocity, there is no mutually assured destruction, there is no deterrent for a nonstate actor to do something bad to the United States on a grand scale, because we would have no answer. If they came from Syria, we are not going to nuke Syria. If they came from a bad part of the world and they were nonstate actors, there is nothing we can do back to them as a deterrent. And these are people that will kill themselves and blow themselves up to kill 20 Americans, let alone 20,000 Americans.

So I guess my question is this. Do you see—and this is for everybody—do you see a weapon of mass destruction going off in the United States as inevitable in the next 25 years? Do we need to get right of the boom, as opposed to left of the boom? We talk about getting left, going out as far as we can for the materials and everything. But do you think that it is inevitable that you will have a device go off at some point in the United States by a nonstate actor, and there is nothing we can do about it? So that is my question.

Dr. BRASURE. I will begin to attempt to answer that question. I would say my answer focuses on we are doing everything we can to prevent that from happening. So in my world, my strategy, our teamwork is designed to prevent that by taking a holistic, risk-based, and multifaceted approach to securing the materials domestically and abroad, as well as setting up the detection and interdiction infrastructure to preclude that from actually occurring.

I would also say that I cannot speak for the consequences, but what I can speak to are the technical capabilities in the national technical nuclear forensics arena, and I will assure you we are developing and we have a capability that we continue to improve to attribute the either interdicted materials or, with our interagency colleagues and some of the other programs, a post—you know, right-of-boom event to actually do the attribution to find out the source of the material.

And so, I would say between those two elements, with respect to the prevention as well as the very real threat of an attribution through various means, including technical nuclear forensics, that again we strive to avoid that scenario from happening in the next 25 years and beyond.

Ms. HARRINGTON. If I could add briefly to that, Mr. Garamendi mentioned the biological threat in his opening remarks, and that certainly is a very serious one. But unlike biological and chemical and even conventional explosive threats, where the material to make a weapon is so ubiquitous that it is difficult to control, in our universe it is all about the material. Without the material, nothing happens.

And you can have all the expertise and all the accompanying technology you want, but without the material, the damage doesn't happen. So our focus is, first and foremost, identifying where the material is—and that, as we discussed yesterday, is an issue between us and the intelligence community, but that is a very close collaboration; identify what the opportunities are to either eliminate the material, preferably, all together, or if not eliminate it, secure it.

If we can't secure it, then make sure we have a detection ring around that material or around that country to give us the highest level of confidence that we will see that material move if it is out of regulatory control. It doesn't necessarily mean it always will be stopped, but as long as we know that something is in motion, then we can work with our partners, you know, in the United States in ports around the world, because of the partnerships we have developed, for that early warning system to kick in.

But that is why it is so absolutely critical to push this protective ring that we are developing as far beyond our borders as humanly possible.

Mr. HUNTER. That is all I have got. If no one else has an answer to that one, I am going to recognize Ms. McSally.

Ms. MCSALLY. Thank you, Mr. Chairman. So I just want to scope the threat again, just—based from your testimonies. So we know there is, you know, basically 30 countries that we are working with, or are available for nuclear material as source, 100 with radiological is what you mentioned. We have got a very active black market, as you all mentioned. According to some open source reports, since December 31, 2014, there have been 2,700 cases reported to the IAEA [International Atomic Energy Agency] voluntarily by 100 countries of illicit trafficking of nuclear and radiological material. So those are the ones that are voluntarily reported.

Just, you know, one example, again, from an article in Moldova, in 2011 an informant was able to buy a highly enriched uranium in a green sack out of a Lexus parked near a circus in Moldova's capital. This is just an example of the challenge that we are dealing with.

ISIS is now present in—with affiliates, organized affiliates—in at least 20 countries, with foreign fighters coming from 120 different countries from all over the world. So this is just scoping the challenge.

You talk about partnering with countries in order to make sure we are preventing on the outer ring. So, in my mind, if—who are the—I guess I would think Russia would be a big challenge. I think Moldova is a country of concern. So, in your expertise, who are the most challenging countries for either lack of capacity, lack of posi-

tive control, or lack of partnership that we are talking about here for source of material?

And I don't know if—whoever wants to answer it, Ms. Harrington or Dr. Brasure.

Ms. HARRINGTON. Well, let me try to answer that in an unclassified way.

One of the big challenges that we confront is, again, the shifting nature of the challenge. So in the past, we have been extremely focused, for example, on the very large stockpile of defense-related material in Russia. And we invested over 20 years of cooperative activity. We feel that, as a result of that cooperative activity, the standards and the practices were improved significantly.

We don't have insight into how those are being sustained any longer, and that causes us concern. But in response to that we have significantly accelerated—and I would say done so with a number of other partners, our European colleagues, Japan, Australia—we have an organization called the Global Partnership, where we bring funds and pool funds in order to improve these capabilities, for example, in Moldova, in Georgia, Ukraine, et cetera. So those activities are underway, and—

Ms. MCSALLY. So if I hear you, I mean, Russia is a concern now due to lack of cooperation, mostly, lack of insight into what is really going on, whether there is positive control or not. Is that fair?

Ms. HARRINGTON. That is a fair statement.

Ms. MCSALLY. OK. And other countries of concern in the unclassified realm—I mean Moldova—I mean, just looking at an article why Moldova might be the most dangerous place on earth, because of this issue. That is a concern to me. I mean can you just share some other perspectives, whether you can in the unclassified, of the countries of concern?

Ms. HARRINGTON. Well, I would say, in general, we have excellent cooperation, for example, with countries like Moldova, like Georgia, like Ukraine, those perimeter countries, because they don't want this—

Ms. MCSALLY. Right.

Ms. HARRINGTON [continuing]. Material passing through them, either.

Ms. MCSALLY. So that is a good cooperation, but maybe lack of total positive control. But at least they are cooperating with us, right?

Ms. HARRINGTON. Absolutely.

Ms. MCSALLY. OK.

Ms. HARRINGTON. Absolutely.

Ms. MCSALLY. Great. Mr. Owen, could we clarify? In your testimony you talked about 100 percent of containers, 100 percent of vehicles are scanned when they are coming in to the country. But you are talking about the radiological scanning. But the physical, the x-ray scanning, is more like 3 or 4 percent, is what I understand. And concerns about shielding or false positives, and what are we doing to maybe close the gap between what is actually being physically scanned versus, you know, what is being radiologically scanned, I just want to clarify it.

Mr. OWEN. Right, and that is correct, 100 percent of the cargo does pass through a radiation portal monitor at whichever border

crossing it is coming through. So we do have 100 percent coverage for the radiation scanning. A much smaller subset of those containers that we determine to be higher risk are then sent for an x ray, if you will, a large-scale—different types of intrusive systems to see what is inside the containers.

Those decisions are based on the targeting information that we receive, and our National Targeting Center has a very strong protocol, if you will, where we take not only the manifest information that the shipper provides, the importer information that the importing company will provide, we marry that up with our law enforcement databases, our trade databases, and most importantly, the information that we have from our intelligence community, as well as our international partners. All of those factors will determine that smaller subset, which is about 3.7 percent right now of those containers that we look at for highest risk.

Now, overseas we look at—of that 3.7 percent, about 1 percent of that is actually inspected overseas as part of our Container Security Initiative.

Ms. MCSALLY. Of the 3 percent, 1 percent—

Mr. OWEN. Of the 3 percent, so it is about 1.1 percent overseas before it heads our way, and about another 2.6 upon arrival, so about 3.7 in total.

Ms. MCSALLY. OK, great. My time has expired. Thanks, Mr. Chairman.

Mr. HUNTER. I thank the gentlelady. The ranking member from California is recognized.

Mr. GARAMENDI. I want to thank the witnesses for all of their testimony. There are so many pieces to this puzzle. The outer ring, Ms. Harrington, and the work that you have done there—my colleague, Congresswoman McSally, went into the Russia issue in some detail. Just one additional question on that.

What efforts, if any, are being made to reengage with Russia on this issue?

Ms. HARRINGTON. Thank you for that question. We have never completely disengaged from Russia, particularly in the non-proliferation, disarmament, threat reduction sphere. We have kept some of that interaction alive, mostly through technical exchanges, best practices exchanges, because if the geopolitics ever permit, we, of course, would want to be working with Russia again, not only in Russia but perhaps teaming with Russia to work in other challenging places of the world. We are the two big players in the nuclear world.

Mr. GARAMENDI. Well, having said that, it appears as though the engagement is at a very low level. That is, not terribly active. Is that the case?

Ms. HARRINGTON. It is at a marginal level right now, yes.

Mr. GARAMENDI. What steps are being made to—are being undertaken to enhance the engagement?

Ms. HARRINGTON. In—

Mr. GARAMENDI. Like, when is your next trip to Russia?

[Laughter.]

Ms. HARRINGTON. I have not been to Russia in a while. But we have staff on the ground in Russia, literally, every week. So it is not that we are not present. We—

Mr. GARAMENDI. This issue of engagement with Russia goes way beyond this particular set of concerns. And it seems to me that it is in the interest of Russia and the United States to enhance our engagement at every level: parliamentary, military, nuclear, and the rest. And so I would encourage you to get on the airplane.

Next question, Mr. Owens. And maybe this goes beyond you to Dr. Brasure also, and that has to do with the secure freight initiative, which was at one point in six ports, and now appears to be only one port. Could you describe that situation, and why it has gone from six to one? And should it be more than just the port in Pakistan?

Mr. OWEN. Yes, absolutely. Back in 2006, 2007, we began to explore the idea of 100 percent scanning, where you would have the radiation screening as well as the x-ray screening before the container was put on the ship. We piloted this in six locations. We were in Qasim, Pakistan; we were in a terminal in South Korea; a terminal in Hong Kong; Port of Cortes, Honduras; Salalah, Oman; and in Southampton in the U.K.

Lots of different challenges that came up from the diplomatic, to having our personnel overseas. There were environmental issues, there was the biggest, which was the throughput of the cargo and the impact at having 100 percent x raying would take place.

The way these two systems work, the passive scanning of radiation is very—quite simple. The container passes through. If there is any radiation emitting, the technology will detect that. The challenge becomes with the x raying of the cargo, because that is a very manual process. Using the different technologies, an operator has to do different things to try to see if there is a threat. And that will slow down the process of the cargo flowing through the ports.

When you have gate traffic—and some of these ports we piloted in it was all gate traffic, so the cargo all arrived at an entry gate in—you can set up a suite of technology that will allow you to perform 100 percent scanning, realizing there will be some impact.

However, in most of your largest container ports around the world, it is transshipment ports. You have ship-to-ship, barge-to-ship, rail-to-ship, which presents a whole other challenge in terms of the flow of the cargo. So, after 4 years of testing this, we documented all of the different challenges, again, along the diplomatic, the operational, the impact, the limitations to the technology, and we decided that we would continue in the places that offer the greatest strategic benefit, that being Qasim, Pakistan—68,000 containers last year that came out of Qasim. Every one of those was scanned for radiation and an x ray was performed, the data being sent to our National Targeting Center here, in Virginia, where a U.S. CBP officer makes that go/no-go decision if that cargo is loaded on the vessel.

In the last year we have also expanded that same operation to Port of Aqaba in Jordan for obvious reasons. So that is the approach that we are taking. Where can 100 percent scanning add the greatest value to enhance our overall security overseas?

Mr. GARAMENDI. And that takes us to yesterday's hearing on the classified—

Mr. OWEN. Yes, sir.

Mr. GARAMENDI [continuing]. Piece of it. Good.

A question to all of you, and that is resources, as in money. And I would like all of you to address this issue of funding, which is our problem. Do you have adequate funding to carry out the tasks that you have been assigned? Let's start with the Coast Guard.

Admiral FAGAN. Thank you. As you know, the Coast Guard participates in this mission from a layered approach. And as you go from the overseas international arena into the offshore, the approach is in the transit zone, and you know we are engaged in a major recapitalization of some of our aging cutter fleet designed to deploy exactly into those approaches in the—thinking specifically of the offshore patrol——

Mr. GARAMENDI. I don't need to hear all the task of the Coast Guard. The question was do you have adequate funding for this specific task that we are discussing today?

Admiral FAGAN. We are doing everything that we can within the mission zone with the resources that we have today.

Mr. GARAMENDI. Well, you danced around the answer. The answer is not appreciated. Either you have adequate funding or you do not. If you do not, we need to know. I mean that is our job. It is our job to provide the funding necessary to protect America, and your job is to carry it out. And right now your job is to answer the question. Do you have adequate funding to carry out this specific task?

Admiral FAGAN. We have adequate funding to carry out the task——

Mr. GARAMENDI. Very good.

Admiral FAGAN [continuing]. As Coast Guard.

Dr. BRASURE. Yes, sir. We also apply the resources we have. And in DNDO we apply them using a risk-based strategy across all areas. And we support the President's budget submission.

Mr. OWEN. And we have a workload staffing model that identifies the resources that we need, and the resource staffing model shows that we are 2,107 officers below what we need to carry out the resources. About 500 of those are directed towards seaports. So, on the personnel side, we do have a model that has been validated by independent groups that show we need additional resources, about 500, for the seaports.

Also concerned about the aging technology that we have in our ports of entry, as well.

Mr. GARAMENDI. Thank you.

Ms. HARRINGTON. We have adequate funding for the mission requirements, but I would point out that affecting the budget of one piece of this layered defense affects how everybody is able to implement, because this is really that integrated. So, if the Coast Guard or Customs and Border Protection, or particularly DNDO is affected in the budget world, then that has an impact on our ability to execute.

Also, I don't want to get into this—it is as painful for Congress as it is for us—but CRs [continuing resolutions] are not a good way to plan and execute programs.

Mr. GARAMENDI. Thank you. I yield.

Ms. MCSALLY [presiding]. Thank you. The Chair now recognizes Mr. Gibbs from Ohio.

Mr. GIBBS. Thank you, Chairwoman. I represent the Great Lakes region, and I realize ports are their major economic drivers, and understand it is important to make sure of port security.

I want to talk a little bit about container security. In 2010 there was a GAO [U.S. Government Accountability Office] report that said that some countries are reluctant to comply with the international port security code due to concerns over sovereignty. And can you kind of give us—any one of you, I guess—this international port security is now—is it uniformly followed by our U.S. trading partners, or is there still concerns with sovereignty?

Admiral FAGAN. The—as I mentioned in my opening comments, the—one of the programs the Coast Guard operates is the International Port Security Liaison Officer Program, where we have visited 150 countries and 1,200 ports, and have generally found quite good compliance as we have made those visits. There have been a small number of ports that have not adequately met that international standard, and we have protocols in for identifying those countries and increasing the scrutiny, the inspection, and the screening regime for ships that would have called from those particular ports.

But generally, compliance is generally good with a few small exceptions.

Mr. GIBBS. What kind of numbers on an annual basis that, you know—that—ships been refused entry or—you know, what is kind of—how often has this occurred, it is a problem that they are not in compliance?

And then also, you know, what—is there a particular country or area that has been more of a problem for clients?

Admiral FAGAN. I will get you the specifics on which countries and what numbers of ship arrivals we experienced from those countries. This is part of the advance notice of arrival screening process. The last five ports of call we look at crew, you know, passengers, containers, part of the National Targeting Center—the Customs and Border Protection mentioned we have a Coast Guard contingent over there. It becomes part of a seamless screening process, looking at the risk profile of a vessel before it comes to the United States, and decisions are made as to whether that vessel needs to be boarded offshore, allowed in port. Again, looking at the totality of the risk profile.

I can get you specifics on what number of ship calls we have had, particularly from the countries that have had a port that is problematic from a compliance—

[The information follows:]

If a country is found to have poor implementation of the ISPS code's security recommendations, it may be considered by the Coast Guard as having inadequate antiterrorism measures and as authorized by law, the Coast Guard may impose conditions of entry (COE) on vessels arriving from that country or a particular port or facility. Such vessels are subject to a range of port State control actions, beginning with a COE verification of their security measures to mitigate risks, up to and including denial of entry.

In 2015, 8,925 individual foreign vessels from 81 different flag administrations made 73,752 port calls to the United States. The Coast Guard conducted 1,712 COE verifications. In 2015, the bulk of the COE verifications were aboard vessels that visited Venezuela, Nigeria, Cote d'Ivoire, and Equatorial Guinea in their last five ports of call before arriving in the

United States. Of the 1,712 COE verifications, 24 vessels were issued “denial of entry” operational controls. None of the 24 were issued due to the vessels’ noncompliance with the COEs, or due to noncompliance with the ISPS code.

With regards to ISPS compliance (not COE), there were 15 “IMO-related” denial of entry operational controls since the ISPS code was adopted. Only one was recorded as being issued to a vessel for failure to implement the ISPS code. That occurred in 2011.

Mr. GIBBS. But you feel pretty comfortable that the program is working, that compliance with our trading partners is improving? Or is there something we can do more to enhance that?

Admiral FAGAN. No, the program is quite mature and is working quite well, and I am very comfortable with the interagency coordination and communication that occurs as that vessel approaches the United States, and that there will not be a—sort of no surprise when a ship actually arrives then in the U.S. waters with regard to what the potential risk profile—be it from a last port of call that may have had a compliance issue.

Mr. GIBBS. Thank you. I yield back, Chairman.

Ms. MCSALLY. The gentleman yields back. The Chair now recognizes Ms. Hahn from California.

Ms. HAHN. Thank you. I appreciate us holding this hearing today. Port security has really been my top issue since I have come to Congress. I represent the Port of Los Angeles and the complex of Long Beach in Los Angeles is within my backyard. So, as America’s port, you know, representing almost—you know, it depends. Using around 42 percent of all the trade coming into this country comes through our ports; Todd and I have worked together on a number of issues.

But I will tell you, since 9/11 my concern has really increased in terms of something happening at one of our ports. Because of the nature of 9/11, certainly Congress has been more focused on aviation security because that was the nature of the attacks that day. And I think we have done a pretty amazing job at really changing the way we behave, and changing the way people fly.

But I really believe that we have not done the same for the ports in this country. I take it very personal and very—I am very responsible about keeping the people of my district safe, but also understanding what an attack at one of our ports would mean to our national and, dare I say, global economy.

I was happy 2012 that my legislation called the GAPS Act [Gauging American Port Security Act], which would have required DHS to identify remaining gaps in our Nation’s port security, passed the House. And in last year’s appropriations bill, my amendment requiring an assessment of cybersecurity risks at our Nation’s most at-risk ports was included and passed. And I am looking forward to seeing the findings that are going to come out in August of that report.

And I am hoping, after today’s hearing, Congress will also seriously take into consideration my other bill called the SCAN Act [Scan Containers Absolutely Now Act], which would create a pilot program to test the implementation of 100 percent scanning technology at two selected ports in this country.



And Todd, I am going to direct my questions to you. It is a little disturbing when you keep saying 100 percent scanning, because that is really not the intent of the law that Congress passed in 2006 called the SAFE Port Act [Security and Accountability for Every Port Act]. That was 100 percent scanning using radiation and x ray. So for you to keep saying 100 percent scanning of all containers coming in our ports is really not accurate, and I wish you wouldn't say that, because it makes people believe that we are following what Congress intended.

And it was unfortunate that Secretary Jeh Johnson has said 100 percent screening and scanning is not the best use of taxpayer resources, and they are delaying yet again Congress' will by another 3 years.

You know, the CBO [Congressional Budget Office] estimated that meeting that mandate would cost about \$22 billion to \$32 billion over the course of 10 years, but we know—and that seems like a lot of money, but we know in 2002, when the west coast ports locked out the workers, we finally quantified that it was a \$1 billion- to \$2 billion-per-day hit to our economy. That lockout lasted 10 days, so there is your \$20 billion right there. And if something were to happen at one of our ports, I think the economic risk, not to mention the loss of lives, would be enormous to this country.

Let's say—you know, I really want to know what you think about—because people say—you are included—most everybody here said it would slow down commerce if we did 100 percent scanning the way Congress intended. But I have never seen that to be proven, one way or another. And my bill would say, fine, let's test it at two ports. Let's have 100 percent scanning, radiation and x ray. Let's see. Because I believe there is technology that exists today that will accomplish both, that will keep us safe but will not slow commerce down.

If Congress decided to pass my bill, and we had a pilot program at two ports, what do you think—is there—do you think there is equipment that you would recommend that we could purchase or could use in testing this thing? I want somebody to prove me wrong, because I don't think I am wrong on this one.

Mr. OWEN. Well, again, with the—the way the law defined 100 percent scanning, it was the radiation and the x ray.

Ms. HAHN. Right.

Mr. OWEN. The radiation piece is doable, we are already doing that.

Ms. HAHN. Right.

Mr. OWEN. We are doing that all around the world. It is the x-ray piece.

Ms. HAHN. Right.

Mr. OWEN. I have not seen a piece of x-ray technology that has yet to offer automatic anomaly detection. Every piece that I have seen still requires intervention from an operator to identify where the anomalies are, and that takes time.

As you know, Los Angeles, Long Beach, 13,000 containers a day. Under your act we would scan and x ray 13,000 containers a day. U.S. Customs and Border Protection currently has 10 pieces of non-intrusive inspection equipment to do that. We cannot do 13,000 containers a day in Los Angeles with the equipment that we have.

So I think it is still an issue of the technology——

Ms. HAHN. Do you think there is technology out there that could solve this problem that maybe you have not tried yet?

Mr. OWEN. I have not yet seen technology that can solve the problem. I know the vendors are working towards technology that can solve the problem, but I have not yet seen it deployed or in an operational setting, where it would not add to the further congestion of the ports. So I think that is something we need to keep in mind, too.

You mentioned the \$22 billion to \$32 billion that the CBO report last month mentions. That does not include the reciprocal costs if foreign governments require the same actions in our ports. So if we had to scan every container leaving the U.S. to go foreign—because that is the requirement we have placed on them—I would argue there would be a detrimental impact on the throughput of the commerce through our ports, as well.

Ms. HAHN. You know, and I know my time is up, and—but, you know, I will tell you I just don't buy that. And I am sorry, and I will say every single day that I think our ports are some of our most vulnerable entryways into this country. And until we act on what Congress decided, 100 percent scanning, I don't think we are going to have the safety and security we need. And I think slowing down commerce is certainly not my first option, but the alternative, what would happen to slow down commerce in this country, nationally and globally, if one of our major ports were to have an incident that shut them down, is unthinkable to me.

And I hope we move forward with 100 percent scanning some day. I think that that should be our goal. I think we should move toward it. And I think there is technology out there. And the more, by the way—and this is my last statement—but the more, by the way, we begin to agree to that goal, we are opening up a great opportunity for entrepreneurs and businesspeople to begin developing technology. But as long as we are shutting the door on that market, I don't think we are going to see the kind of technology that I know we are capable of creating to do both, keep us safe and move commerce.

Thank you very much for the extra time. You know my passion about this.

Mr. HUNTER [presiding]. I thank the gentlelady. And our next panel is going to be a bunch of super-smart people on technology. So I hope you will stick around for that.

With that, Mr. Curbelo is recognized.

Mr. CURBELO. Mr. Chairman, thank you for this opportunity, and I thank all the witnesses for coming this morning.

Admiral, a question for you. What is the Coast Guard doing to monitor potential risk from small-vessel attacks in U.S. ports, and distinguish between legitimate vessel operators and those engaged in illicit activities? This is of particular interest to us in south Florida. We have many small vessels in our waters. Please, go ahead.

Admiral FAGAN. Thank you. As you know, the small-vessel threat is exceedingly complex, and there is no one single agency that can, you know, counter the threat from small vessels and, you know, constant vigilance is a—is an important element in the small-vessel threat realm.

Within the ports—and I can speak specifically from my time as the captain of the port in New York—there are a number of, you know, coordinating and communicating mechanisms through the Area Maritime Security Committee and others that help bring the other entities together to look at and understand what the risk and the threat streams may be.

I am confident that within the law enforcement and the intelligence information flow into those coordinating communicating mechanisms, that we have got a whole-of-government, including Federal, State, and local partner, look at this threat stream, as well as others that may confront a port community in the United States.

Mr. CURBELO. So it seems a daunting task to track small-vessel activity. Can you get into the degree of coordination you have with local authorities to help extend the Coast Guard's reach and really monitor this as much as possible?

Admiral FAGAN. Yes. So the Coast Guard coordination—you know, we have talked about at the international level, I will talk very specifically now at the port level. And again, to my personal experience in the Port of New York, there were over 200 agencies that we were regularly coordinating and communicating with. There are daily phone calls with some of the key law enforcement partners and agencies to get at and share information exactly on threat streams, small vessels or otherwise.

That level of information and collaboration and coordination has never been better. There are other—you know, whether AIS [automatic identification system] and other technical means that then also allow insights into the number of vessels that are out there, and where that threat stream may be. Intelligence and law enforcement information really become powerful enablers as we look to counter threats from small vessels.

Mr. CURBELO. Also your testimony states the Coast Guard conducts over 400 routine inspections in general law enforcement boardings every day to ensure vessels comply with international maritime law and safety standards, applicable U.S. law and regulations, and any control procedures required to access the Nation's ports.

Well, what are the infractions that are typical of one of these boardings or inspections?

Admiral FAGAN. So if it is a large commercial vessel, we have talked about the screening, the advance notice screening. The infraction could be denial of entry into the United States of the vessel. The captain of the port has a broad range of authorities and responsibilities, and would be well within that individual's authority to prevent a vessel from entering, to hold a vessel in port requiring certain safety and security and environmental compliance regulations be met before that vessel moves, all the way down to—and in the small recreational vessel community it could be a violation for failure to carry lifejackets. It runs the full breadth of safety, security, environmental, and the sort of follow-on actions are commensurate with what—

Mr. CURBELO. Do you have a rough estimate of how many of these approximately 400 daily boardings are small vessels?

Admiral FAGAN. I do not have it, but I can get that for you—

Mr. CURBELO. Sure.

Admiral FAGAN [continuing]. Exactly what, you know, the number of large-vessel boardings, the small-vessel—what we call a 4100 boarding, how many of those are occurring each day. And I will provide you a more detailed breakdown.

[The information follows:]

The Coast Guard averaged over 400 boardings or inspections per day in FY15. The below table includes confirmed boardings of small (less than 300 gross tons) and/or recreational vessels, large (greater than 300 gross tons) vessels, and Safety/Security/Compliance Inspections of U.S.-flagged or foreign-flagged vessels.

FY2015	Total	Large Vsl Boardings	Small Vsl Boardings	U.S.-Flagged Vsl Inspections	Foreign-Flagged Vsl Inspections
Annual	157,169	15,512	52,495	56,378	33,079
Daily Avg.	434	42	144	156	92

Mr. CURBELO. Thank you, Admiral.

Mr. Chairman, I yield back.

Mr. HUNTER. I thank the gentleman. Mrs. Torres is recognized.

Mrs. TORRES. Thank you, Mr. Chairman. I want to associate myself with the comments given by my colleague that represents the Port of Los Angeles and Long Beach. I represent the 35th Congressional District. Everything that comes through those two ports makes its way to my district. We have lots of warehouses. Logistics is the business of the district.

So, yes, I am very, very concerned about containers coming through, whether it is coming through the Alameda corridor or it is coming through by truck on the I-10 or the Route 60 freeway, which are regularly overcrowded with commuters trying to make their way to and from their jobs in Los Angeles to the Inland Empire.

It is alarming to me that we have continued to ask for extensions. In this last request to extend this 100-percent check, is this your last request? I mean what assurances do we have that you actually have the technical expertise to deliver on your promise to Congress that you could meet the requirement given?

Dr. BRASURE. So what we are doing in response to the Secretary's new look at the legislation is to—we have put out an RFI, request for information, to look broadly at both material and non-material solutions to the 100-percent overseas scanning. And we received—we targeted not just technology solutions, but broadly look into the private sector, for instance, to gain their insights, port operators, trade unions, just broadly and innovatively across the overall enterprise.

We received approximately 30 responses back last month, and my team at DNDO is right now evaluating those responses. And indeed, they came from not only technology companies, but all the entities I just mentioned, they responded.

So, once we evaluate those, we expect to hold meetings in sessions with the successful respondents in the August-to-September

timeframe, and we would be happy to come back and brief you on——

Mrs. TORRES. So these 30 new responses, they are different from what previously you have received? And how are they different?

Dr. BRASURE. So they are different because we looked, again, more broadly beyond technology companies. And I would like to point out that, with respect to technology companies, we are currently piloting and evaluating technologies that could be applied to 100 percent scanning, and we are in various stages of evaluation in pilots for such technology solutions.

But again, the RFI is addressing more broadly inputs from, again, the private sector and looking to them for their solutions, and they are sharing in this 100-percent scanning activity.

Mrs. TORRES. Rear Admiral, in your testimony you state that the Coast Guard conducts foreign port assessments and have visited more than 1,200 port facilities. Does the Coast Guard share those results of the security assessments with U.S. ports, such as the Port of Los Angeles and the Port of Long Beach?

Admiral FAGAN. So the outcome of those port visits and port assessments factor into our risk-based screening, as we determine what the risk portfolio around a large commercial—presenting to the United States from a passenger and cargo and crew standpoint, and that is then factored in to, you know, the decisions on whether you are going to do boarding offshore at the anchorage, or into the port.

In cases where there is a particular concern, say, with a crew-member that you are concerned may get off the ship, there are then, you know, additional security measures that are coordinated, you know, through the Coast Guard and the captain of the port authorities. I am not sure how much is publicly shared in the unclassified realm, but I do know it is very fundamental to our valuation of risk associated with a ship because of having called at one of those——

Mrs. TORRES. I am more concerned——

Admiral FAGAN [continuing]. A port that might not——

Mrs. TORRES [continuing]. Ma'am, about sharing lessons learned, you know, what you are learning about potential risks, not necessarily attached to, you know, personnel, but logistics types of risks, where we could do a better job sharing information with the port authorities, as well as—I want to make sure that you are including—and this is for all of you—don't forget that, you know, the shipments that you are not inspecting eventually make their way to districts like myself, putting millions and millions of people at risk.

And I think, you know, we really need to look at and consider what is the life—the cost of the lives of these millions of people that are being put at risk when we fall down and continue to ask for extensions? I understand, you know, that there are technical challenges, but at some point we need you to deliver on what Congress has asked you to do.

And with that I yield back.

Mr. HUNTER. I thank the gentlelady. And I would like to point out, too, to Ms. Hahn, we have the RFI that the Department of Homeland Security has put out to—an open RFI that said, “Hey,

come one, come all, bring your technology, bring your best stuff, we want to see it, we want to do this," right? It is right here. If anybody would like to see this, too, we have it on hand.

Ladies and gentlemen, thank you very much for your time, for your service to our Nation, and for doing what you do. Because without you we wouldn't have—we would not be as safe as we are now. And I just hope that you are always seeing the new challenges coming up and—especially when, once again, when people will kill themselves to kill 20 Americans, they will happily sacrifice their lives to Allah to kill thousands of Americans. I think that that raises the stakes. Like Ms. McSally said, when you put in—when you combine terrorists with weapons of mass destruction, it is a whole new ball game. And that is where we are right now.

So thank you very much, and we can have our next panel of witnesses come up. Thank you. And I will go ahead and introduce them now.

On our second panel of witnesses, Ms. Jennifer Grover is the Director of Homeland Security and Justice for the U.S. GAO. She will be the first to present testimony. Then we have Dr. Gregory Canavan, a senior fellow of the Los Alamos National Laboratories; Mr. David Espie, the director of security at the Port of Baltimore; and the final witness, Mr. James Weakley, president of the Lake Carriers' Association.

And I would like to preface this next panel. I would hope that everybody that was on the next panel was present here during the first panel. And if you could, let's talk about what we just heard. We had a classified hearing yesterday, we just had this hearing now, and you just heard how our Government offices are trying to treat any kind of weapons of mass destruction, from the far-flung areas of Moldova and Georgia and Ukraine all the way to our shores, checking small boats and also checking with other countries and having them help us by checking stuff as it leaves their nations.

So, Ms. Grover, if you would start, and I don't necessarily have any questions specifically for this panel, but I would like you to comment on what you just heard. Because, I mean, that is the American security system you just saw for weapons of mass destruction. They were just here, they just talked, so I am curious what your take is. Thank you.

**TESTIMONY OF JENNIFER A. GROVER, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; GREGORY H. CANAVAN, PH.D., SENIOR FELLOW, LOS ALAMOS NATIONAL LABORATORIES; DAVID A. ESPIE, DIRECTOR OF SECURITY, MARYLAND PORT ADMINISTRATION, PORT OF BALTIMORE, ON BEHALF OF THE AMERICAN ASSOCIATION OF PORT AUTHORITIES; AND JAMES H.I. WEAKLEY, PRESIDENT, LAKE CARRIERS' ASSOCIATION**

Ms. GROVER. Yes, sir. Good morning, Chairman Hunter, Chairwoman McSally, Ranking Member Garamendi. I will focus most of my comments today on the perspectives that you heard from CBP.

With about 12 million cargo shipments arriving each year, the U.S. maritime ports do indeed remain vulnerable to smuggling. CBP has determined that it does not have the resources to examine

every shipment. So, instead, what they are doing is counteracting the smuggling threat by identifying and examining the high-risk shipments. Yet, ensuring that this approach functions properly is indeed still a work in progress.

So, I will focus on two points. First of all, how does—how well does CBP do in identifying those high-risk shipments for examination? And then, secondly, how well do they do in actually examining the high-risk shipments that have been identified?

So, the automated targeted system is the heart of CBP's ability to identify those high-risk shipments that could contain weapons of mass destruction, illegal drugs, counterfeit goods, or other prohibited items. The system works by designating every shipment as low, medium, or high risk, based on a broad range of information that is submitted by importers, vessel carriers, intelligence, and other Government and public sources. It is used to identify the high-risk cargo before it is loaded onto vessels at the foreign ports, as well as to identify high-risk shipments approaching the U.S. ports. Thus, it is essential that the system be accurate.

In 2012, GAO found that CBP updated this system without evaluating the impact of the update on the accuracy of the targeting. At the time, CBP's data on its targeting accuracy suggested considerable room for improvement. Specifically, of all the shipments found during examination to include contraband, such as guns or drug shipments, only 6 percent had been identified by the targeting system as high risk. Now, this is data from 2011 and 2012, because this was from a 2012 report.

In other words, the remaining 94 percent of shipments that were actually found to have contraband during examination had been identified as low or medium risk by the system. Also, at the time, CBP did not have a target accuracy rate, which was limiting their ability to monitor progress in the area.

Now, last year, CBP responded to GAO's recommendations by setting a target accuracy rate, and by requiring that future system updates should evaluate the impact that it would have on accuracy, as well as on workload. And therefore, they are in a better position to monitor the accuracy, going forward. And I can tell you that the targeting accuracy rate now is significantly improved over where it was in 2012, and the component continues to refine the targeting and the method for analysis.

So now let me just take a minute or two and talk about how well CBP does at ensuring that those high-risk shipments are actually examined after they have been identified. So CBP's policy is that every high-risk shipment must be examined, unless the exam has been waived by a CBP officer. In a 2015 report we found that, of the roughly 120,000 high-risk maritime shipments that are processed each year—that were processed each year, 2009 through 2013, most, about 90 percent, were actually examined.

But CBP did not have good data on the disposition of the other 10 percent that should have been waived. Our review of the data showed that some of those shipments weren't actually high risk, so they would not have needed to be examined. Some were examined and recorded improperly, but there were some that were not waived, but also not examined, in violation of CBP policy. And among those that had been waived, we found that the CBP officers

varied in their understanding of the waiver categories and criteria, which could lead some shipments to be examined unnecessarily in a waste of resources, and other shipments waived that should have been examined.

So, we made several recommendations which CBP has addressed. They have new guidance and policy that should enhance consistency across CBP officers, thus leading to greater assurances that all of the high-risk cargo will either be examined or waived, as appropriate.

So just one or two other points on some of the issues that came up today, and that is to acknowledge that maritime ports are indeed vulnerable to smuggling by means other than cargo containers.

Small-vessel securities was one of the topics that was discussed by the previous panel; that does indeed remain a challenge because small vessels are unregulated. They are just hard to track.

Another example of a different type of vulnerability besides the cargo containers is that ports remain vulnerable to illegitimate access through weaknesses in the TWIC [Transportation Worker Identification Credential] access card program, which is the way that—the system that is used to control access to the ports.

So DHS does have multiple initiatives in place to address both of those issues. They are aware of the concerns, and they are making progress, although more work needs to be done.

So, to conclude, DHS does indeed have multiple systems in place intended to ensure port security, to identify and examine cargo shipments at high risk for smuggling, but in this area of Government operations, as in many others, it is essential that the Department implement the programs as intended and, very importantly, monitor outcomes to maximize security.

Thank you for the opportunity, and I look forward to any questions you may have.

Mr. HUNTER. Thanks, Ms. Grover.

Dr. Canavan, good to see you again. You are recognized.

Dr. CANAVAN. It is nice to be back. I am here to talk about the detection of clandestine nuclear weapons.

The last time I was here I made the argument, which I think has held up pretty well, that fast neutrons could be used to detect bare nuclear weapons in things of the size of, say, a TEU [twenty-foot equivalent unit] or two TEU, for weapons that were in with a manifest of ordinary things, normally in one of those containers. This time I want to extend that to say I believe that the same approach can be used to detect nuclear weapons which are in TEUs, but instead of just the bare core itself, something with a basketball size of moderator or absorber around it to minimize its signatures to make it harder to detect.

I am talking about nuclear weapons rather than the dirty bombs which have been primarily discussed up to this point. And I am emphasizing weapons, because nuclear weapon material—uranium or plutonium—has essentially no useful and reliable signature that can be detected passively. Uranium and plutonium have a few gammas that are easily screened out by a thin layer of lead. So you really do need to do something to excite the system in order to get



a signal out—in this case a fission, a unique and discernable signature that leads to high-confidence detection.

I am sorry Ms. Hahn left, because it is also a very fast detection system. It has a very low false alarm ratio. Therefore, it would be suitable to inspection of everything that goes through a port, rather than just a fraction of it, because it is fast and doesn't have the false alarm problems for reasons that I will come back to in just a minute.

It is largely the same story as the previous testimony. Fast neutrons scatter around inside the container. If they encounter nuclear material, they produce fission. The fission neutrons diffuse out as a distinct and pervasive signal that is easily detected.

The reactions that produce the fission neutrons produce a big separation in energy between the source neutrons and the fission neutrons, which is the basis for high signal-to-noise ratio detection. Filtering between the two energies detects the signal.

A couple of quick points. One is that the fast neutrons penetrate a large portion of material to produce this direct signal. Even when something is buried in an enormous amount of moderator, the high signal return from the moderator itself still reveals the composition and thickness of that moderator, which signals the object's intended purpose.

A related point that I thought would have come up the last time, but didn't, is that when someone puts additional moderator around a weapon to hide its signature from the weapon, that increases its signature and criticality.

As an example, if you take a solid-core device, the kind Pakistan has put into international commerce now, back off about 10 percent margin for safety, but then add another 15 centimeters of moderator around it for signature reduction, you return it right back up to criticality. That won't hurt us, but might be a problem for the person who assembles it at the point of origin.

A related point is that when you put fast neutrons into a nuclear assembly, it produces fewer fast neutrons than you put in. So you cannot generate a critical assembly, or a nuclear explosion, by nuclear interrogation itself of a subcritical device. So that is not an additional concern.

A related point is that when you interrogate a nuclear assembly with a moderator around it, the neutrons bounce back and forth between the core and moderator and produce fission many times. The net result is that you get a signal that persists many—10, 100—times longer than the length of the exciting pulse. It is a distinct signal with high energy that persists for long times and propagates long distances from the device.

A technical point is that the detection on the basis of energy depends on the ratio of the difference in energy between the fission and the source neutrons divided by their variance. I am sorry, this is statistics 101, I can see you are not appreciating this, sir. No more math, no more math.

[Laughter.]

Dr. CANAVAN. But the point is that fission produces a big energy separation, and for fundamental reasons, the variances of the fission neutrons become smaller in time as they go down in energy. Their signal-to-noise ratios get to be 100, 1,000, 10,000. With very

high signal-to-noise, you have very low false alarm ratios, which is what Ms. Hahn was alluding to.

And so, it is everything that you would like to have. Plus, as it turns out, the way the statistics go together, the high signal-noise ratios that you generate are quite insensitive to the statistics of the noise, so the signals remain exceedingly high.

To put this into context, x rays can tell you that there is mass, but can't tell you what it is. Passive sensors can't detect nuclear materials with low signals. There is nothing to detect. And thermal neutrons, which is what the DOD [Department of Defense] spent most of its money on after 9/11, produce complicated detection schemes with low statistics that are easy to counter measure.

Overall, fast neutron interrogation offers an approach that would fit well with the sensors and mountings for these existing systems, and would produce what I think is an exceedingly high signal noise, low false alarm, high throughput system, based on fairly straightforward physics that is used in reactors and experiments every day, sensors that are used today for down-hole well-hole logging, and detectors that are used for reactors and experimental physics for measurements are made at fairly low and benign energies.

Thank you very much, sir, and I am sorry about the math.

Ms. MCSALLY [presiding]. Thank you, Dr. Canavan. I am having flashbacks to my physics classes at the Air Force Academy. I won't sleep well tonight. But we got some good questions based on the technology that you discussed.

And Mr. Espie, you are now recognized for 5 minutes.

Mr. ESPIE. Thank you, Chairmen Hunter and McSally, and Ranking Member Garamendi, for convening this hearing today. I am testifying today through your invitation, and on behalf of the American Association of Port Authorities, where I am a member of the Security Committee. This is a vital topic, which could ultimately impact the safety and security of the United States if not addressed in a cohesive and expedited manner.

In my role as director of security for the Port of Baltimore, the prevention of maritime nuclear smuggling into the United States is a top priority, and it requires a multifaceted approach. It requires the input of diplomatic resources, technical assets, human capital, and appropriate funding to facilitate subsequent preventative methodologies. All this requires a strong partnership with the Federal Government.

As a retired FBI agent and former special agent with the National Security Agency, I also view our security from a national and international perspective that must empower ports to be more engaged in our national security apparatus. In my experience, it is vital that our Government have sound diplomatic relationships with countries that will cooperate with the United States in not only applying necessary security measures to secure their own nuclear materials, but will also assist in countering a neighboring country or one in the certain region that may possess such material and may have negative intentions against our country and others.

Global diplomacy and policies impact local port security enforcement. Positive measures currently in play are the State Department's Counter Nuclear Smuggling Unit, the Department of Ener-

gy's partnership with nearly 50 countries providing radiation detection and nuclear forensics equipment, and the recent Nuclear Security Summit held here in Washington.

I cannot emphasize enough the importance of technical aspects of our intelligence and Federal law enforcement agencies that must be continually deployed and refined.

Existing capabilities and resources must be deployed and fully capable in order to maximize our country's opportunity to readily identify and neutralize potential threats. Development and tasking of domestic and international sources must remain a priority for intelligence agencies and services and our local State and Federal law enforcement agencies. In some cases I believe it would be beneficial for our port security directors in the United States to receive FBI briefings.

The threat of maritime terrorist smuggling appears to be increasing, possibly in correlation with the flight of Syrian refugees to and from Europe. Recently, a stowaway on a roll-on, roll-off vessel destined for the Port of Baltimore was located by a ship's crew and taken into custody by CBP and HSI [Homeland Security Investigations]. The stowaway admitted that he boarded the vessel while it was docked at a German port. Approximately 1 week prior to this event, a shipping lines manager in Baltimore advised me that his lines had experienced several stowaway attempts by Syrian nationals in Germany, as well.

Directors of port security in the United States are not routinely granted a security clearance with the Federal Government, and hence are not provided classified briefings regarding threats to their ports. In addition, port security directors are unaware of any type of unique intelligence centers wherein maritime nuclear smuggling intelligence is specifically received and analyzed in an effort to connect the dots, if you will, and prevent such an incident.

The suspects of maritime nuclear smuggling efforts are numerous. The actions and aggressiveness of ISIL, for example, are challenging all aspects of our port security procedures. The threat from ISIL emerges on several fronts. First, the size of ISIL's force is substantial. Secondly, ISIL is not a congruent entity. Its leadership remains in a fractured state and, subsequently, subfractions form that are very difficult to identify or even trace. Third, ISIL's use of the Internet and related systems to recruit both actual soldiers or lone wolves has proven to be extremely successful.

As a former police officer, now as a port security director, resources that can be utilized at the local level are vitally important. FEMA's [Federal Emergency Management Agency's] Port Security Grant Program has been instrumental in coordinating port-specific security needs with national and global threats.

The AAPA [American Association of Port Authorities] encourages Congress to continue to fund the Port Security Grant Program, but also insist that grant funding be directed to ports and not diluted to other law enforcement entities that are not associated specifically with ports.

Cybersecurity is also a prime example of emergency security concerns since 9/11. Ports are working with stakeholders in addressing this very complex issue. For example, in a recent survey conducted by the AAPA, it was found that 52 percent of our ports have con-

ducted a cybersecurity assessment within the last 3 years and 67 of our ports' Area Maritime Security Committees have formed a cybersecurity working group.

Cargo containers have been identified as the most plausible mechanism for smuggling nuclear material into the United States. Over 11 million containers are shipped to our Nation's 300 sea and river ports on an annual basis. With the recent completion of the Panama Canal expansion, the number of containers from foreign ports will dramatically rise.

Congress previously mandated that all incoming containers to the United States be screened overseas. To date, this law has not procedurally been incorporated wherein exemptions have been employed by the Department of Homeland Security. Recently, an extension of the law's implementation was again approved by DHS with the support of the AAPA and by also 100 supply chain industry stakeholders. It has been estimated that it would cost approximately \$20 billion to deploy scanning procedures and technology at the 700 foreign ports which ship cargo to the United States.

And I mentioned containers. This does not cover what we call roll-on, roll-off cargo—RoRo cargo—vehicles. In the Port of Baltimore we receive over a half million vehicles a year. They are not scanned as they come to the United States.

In sense of time, I would just like to go to the conclusion to whereas—again, our—in summary, our Nation's strategy to prevent maritime nuclear smuggling must utilize a holistic approach. This strategy should continue to incorporate diplomatic engagement; utilize the intelligence community, human and technical assets; continue the examination of port security protocols to include those which are federally mandated and those imposed by port operators themselves; increase funding of the Federal Emergency Management Agency's Port Security Grant Program to ensure ports are and remain in Federal compliance; and the investment of appropriate funding levels for Federal agencies, particular CBP, in order for current and future legislative mandates to be properly implemented.

Again, I thank you for this opportunity, and I am glad to answer any questions directly and explicitly.

Ms. MCSALLY. Thank you, Mr. Espie. The Chair now recognizes Mr. Weakley for 5 minutes.

Mr. WEAKLEY. Good morning. There is a tremendous interest in the intersection between our maritime industry and homeland security. Our Nation's water borders far exceed our land borders.

The Great Lakes demonstrate the importance of marine homeland security. The southern land border of the United States is about 2,000 miles long. However, the Canada-U.S. border is three times as long, and much of that is water. I represent 14 American companies who operate 56 vessels on the Great Lakes. We carry the raw material that drives our economy: iron ore and flux stone for steel, aggregate and cement for construction, coal for power, and other cargoes. We transport 100 million tons of cargo a year, and employ 1,600 Americans. Our cargoes generate 103,000 jobs with an economic impact of \$20 billion.

I will focus the majority of my testimony on how my members transition their vessels from homeland security risks to resources.

The Great Lakes are tied together by connecting channels and locks. The St. Lawrence Seaway connects us to global trade. The navigation channel crosses the U.S.-Canadian border 17 times in the Detroit-St. Clair River alone. Canadian and American fleets compete for the cross-lake cargo. In 2013 it was 37 million tons. Canadians carry 93 percent of it; Americans carried only 3 million tons.

Foreign-flagged vessels primarily import steel and export grain via the Great Lakes. DHS warns an interruption of domestic shipping through a single lock in Michigan would have catastrophic impacts on the regional and national economy, and would plunge North America into a severe recession. DHS estimates that 11 million Americans would become unemployed if this lock were inoperable for 6 months. The resulting loss of 60 million tons of cargo would drive Michigan's unemployment to 22 percent, exceeding its peak unemployment rate of 15 percent during the 2009 recession.

The Jones Act is the fundamental law of American maritime industry, and also a fundamental law of American homeland security. It requires that any cargo moving between our ports be carried on U.S.-built, U.S.-owned, and U.S.-crewed vessels. In other words, American vessels. One of the most important benefits of the Jones Act is homeland security, which includes the prevention of smuggling and much more.

Former Senator Slade Gorton wrote, "helping to plug a porous border is a benefit of the Jones Act that is far too often overlooked." The single most important thing you can do to promote maritime homeland security is to support the Jones Act. I have worked for the Coast Guard, for an American shipping company, and now for LCA [Lake Carriers' Association]. I strongly believe the Jones Act is our best line of maritime homeland defense.

Risk is a combination of threat and vulnerability. The Coast Guard uses the MARSEC [Maritime Security Threat Level] system to relay threat levels. Once notified, we take action. The second aspect of risk is vulnerability. LCA members use our Coast Guard-approved alternative security plan to minimize our vulnerability. We deploy many security measures, including access control, perimeter expansion, personnel screening, vessel security sweeps, random baggage searches, inspections of cargo, and inspections of ship stores. We adjust our security profile based on threat level, vessel operations, and operational area.

Professional mariners recognize something afoul, and notify the Coast Guard via the Eyes on the Water program. Shipboard radars can detect and monitor uncooperative aircraft and vessels. We are partnering with a vendor to record radar screens and to allow remote access. Providing historical pictures can reveal suspicious activity. Remote access provides actionable information. These low-cost programs make our homeland more secure. We are proud to be full partners.

Threats to homeland security are daunting. Every day we execute security plans, cooperate with law enforcement, implement innovative programs, and defend the Jones Act.

Our goal, as Americans, is to transition from security risk to security resource. Thank you.

Mr. HUNTER [presiding]. Thanks, Mr. Weakley. It is kind of funny. We were talking about privateering, actually, when James Madison—and how he gave—he basically deputized American merchant mariners to go protect America's shores and ocean, something we are looking at, a little bit tongue in cheek, but not really. I mean, because that is what—in San Diego we had the same thing, where our sport fishermen are out there on the water every day, watching boats going in from Mexico, and they know who is good and who is bad. And CBP relies on them massively because a lot of these guys are former cops, former security specialists, military, and they are on the water every day. So thank you.

Two things. Ms. Grover, one, do you know—has GAO looked at—let's look at this, let's look at 90 percent of what the Coast Guard does in terms of interdicting drugs and stuff and people, compared to what would happen if you have a nuclear device go off. Have you looked at the percentage of resources, time, and assets that are used for a—for homeland security, meaning stopping a weapon of mass destruction, versus all the other stuff that the Coast Guard does?

Ms. GROVER. In terms of the Coast Guard's assets, I believe that the intent was to dedicate about 18 percent of all of the asset resource hours to the ports and coastal waterway security missions. So roughly 20 percent off the top. Now, that would include more than just port security, strictly.

So, for a \$9 billion-a-year organization—that is just the entity part of it, not the personnel part of it, but the people go along with entity, so they—that is a significant area of work for the Coast Guard.

Mr. HUNTER. So 20 percent, then.

Ms. GROVER. About 18 percent, yes, for 2016 was their intent for the resource allocation for the assets.

Mr. HUNTER. I am just trying to balance out the outcome of a weapon of mass destruction going off versus what they—how much time they spend on this. Because if you combine all the other bad stuff that the Coast Guard stops coming in, I was just—in Colombia you have got cocaine flowing in like water to the U.S. Doesn't seem to be any way to stop it. And a lot of the Members that were with us asked a question, "Well, hey, what if we took our focus off the drugs and put it on the weapons of mass destruction? What more could we interdict, and how much safer would we be?"

I am curious if the GAO would look at that at some point in the future, saying if the Coast Guard spends 40 percent of its time interdicting weapons of mass destruction, or trying to, and keeping an eye out for those things specifically, how much does that decrease the probability or likelihood of a weapon like that being put on U.S. soil?

Ms. GROVER. Yes, we would be happy to do that in the future.

Mr. HUNTER. That would be great. I think that is important, because then the Coast Guard could look at what they are doing and say, "Hey, maybe we should spend more time on this."

Dr. Canavan, I guess the big question is this. Ms. Hahn asked—what is the gentleman's name from CBP? Mr. Owens. He said that they have devices, they have technology right now to be able to

look at everything, but not without a human person there, without a person there. And I have seen this stuff.

SAIC in San Diego has got a system that they are selling all over the world—not to us, but all over the world, but it still takes a person there, trained to recognize that that thing—that there is something shielded, that the neutrinos are acting weird around some circular device, or that there's weapons or drugs or—it still takes a person. And I guess their answer is, if you have a person that slows things down massively—that was basically their answer to Ms. Hahn's question was it makes things too slow, it is going to back it up. It is going to be like TSA [Transportation Security Administration] at the airport, but in our ports. And nobody wants that. Nobody wants a TSA in our ports, right? They are doing bad enough already, just with humans, right?

So I guess the question is what exists, if anything, right now, where it doesn't take a person?

Dr. CANAVAN. Well, that is what I am saying. It is unfortunate Ms. Hahn stepped out, because that—

Mr. HUNTER. Turn your mic on, please.

Dr. CANAVAN. Have I done it again, sir? The—that is exactly what I was shooting for, was a system that had a—if you have a very high signal-to-noise ratio, which is what you can get from math that I won't go into here—

Mr. HUNTER. Thank you.

Dr. CANAVAN. Then you have a very low false alarm rate to where you don't have any need for a human intervention. So that is—

Mr. HUNTER. I see.

Dr. CANAVAN. At the top level, that is the answer. The other answer is that whether you use x rays or whatever, the—they are only sensitive to mass. They don't know what the mass is. To them a bomb looks—has the same kind of material in it—as a ball bearing. The reason you have a human operator there to look at these from all different angles, having seen all this many times before, to add human experience, is because you have a lousy signal to start with. All you know is that something bounced a lot of x rays back. With fast neutron interrogation, you actually are stimulating the core of the thing you are looking for to release fission neutrons, which have a unique and specific and high signature, which can't be confused with hardly anything else in the universe.

So you have a great signature to start with, a real signature, and not just some x rays getting bounced around. Plus you have a very high signal-to-noise ratio. That is why the goal that I had was not only to find a nuclear weapon, but to be able to candle everything that went through a port. And I think that is what I have tried to demonstrate in the testimony that I prepared.

Incidentally, I would like to ask that that be submitted for the record. I forgot to ask before.

Mr. HUNTER. Say again. Oh, without objection.

So I think my last thing is I think what the Coast Guard is going to do, and what DHS is going to do, is try to get the 100-percent perfect solution, which will take them a decade. It will take billions of dollars, and they are going to try to be able to find everything from weapons to cocaine to weapons of mass destruction, as op-

posed to just really narrowing it down to weapons of mass destruction, which is what I think they should totally focus on to the detriment of some of the other sectors, like drug interdiction and human smuggling and weapons.

But you are saying that it is possible to not have a human to check for weapons of mass destruction, nuclear devices, with a very low false positive rate, everything that comes in very quickly?

Dr. CANAVAN. Yes, sir. That is what I was shooting at. And like I say, there are two things. One thing is that there is a real nuclear signature from a nuclear weapon. Nothing else looks like it when you hit it with fast neutrons. So the one thing is you have a real signature that you don't with all the others. I am not criticizing what these other groups are doing. You do what you can. If they just have systems that have very indirect signatures, I think they are working very hard to get the very best they can out of that.

What I am saying here is that for reasons that nobody bothered to look at for some reason, there is a system that gives you the combination of a unique nuclear signature and a very high signal-to-noise ratio, low false alarm rate that sort of gets you away from reliance on all of these other signatures that are very indirect.

Mr. HUNTER. What system is that?

Dr. CANAVAN. Sir?

Mr. HUNTER. What system is that? Does that system exist? I mean does a company make that?

Dr. CANAVAN. No. This is my own little research project. Well, maybe I should form a company.

Mr. HUNTER. You want to talk to Gene Ray in San Diego. They have a neutrino system that I have seen tested. They had a lead-encased nuclear device—not a nuclear device, but lead-encased nuke stuff in a car, and they have a system where it does exactly what you say. And they are selling it to other countries, not to us.

Dr. CANAVAN. Well, the neutrinos are nice, but they don't interact very well, and the sources are terrible. But the thing that is popular right now, the closest thing, is muon detection, and that is what a company is testing in Freeport, in the Bahamas.

Mr. HUNTER. Yes.

Dr. CANAVAN. And that works well. But again, it just measures mass, it does not measure nuclear signatures.

And so, you know, I don't want to criticize what other people are doing. You do—you try—everybody is trying to put together a good system, based on whatever we have, which ain't much. After 9/11 it was basically nothing, right?

Mr. HUNTER. Right.

Dr. CANAVAN. So people are trying very hard to do the right thing. I am just saying I think this is a very nice system which, for some reason, we just skipped over. And I would like to see somebody pick it up and do it.

Mr. HUNTER. Thank you, Doctor.

Ms. McSally?

Ms. MCSALLY. Thank you, Mr. Chairman.

Ms. Grover, CBP testified that they are scanning—although there is limitations to that—3 to 4 percent of containers that are coming in, based on their high-risk designation. You just testified



that in the sample that you were talking about from a couple years ago, of the group that they called high risk, it only successfully identified 6 percent accurately to be high risk, missing 94 percent of the actual high-risk containers is what I understood. That is a pretty dismal number.

You since said that they have improved. Are we now at 7 percent and we are missing 93 percent, or where are we right now? That was very disconcerting to hear.

Ms. GROVER. So let's take a minute and talk about this. The 3- to 4-percent scanning, I think what they were referring to is the percentage of containers that are ultimately subject to the x-ray exam, the nonintrusive inspection exam—

Ms. MCSALLY. Right.

Ms. GROVER [continuing]. Right, that takes an image—

Ms. MCSALLY. But their whole briefing and everything yesterday was based on them identifying high threat, high risk.

Ms. GROVER. Right. So roughly 1 percent of the cargo shipments are identified as high risk. And those are the ones that then are required to go through the NII [nonintrusive inspection] so that there is an image that is taken, and the image has to be read by a person.

Ms. MCSALLY. Right.

Ms. GROVER. And the question is then do we unpack the container to find out what this is, or does it look like it is OK and we can let it go through, right? And the procedure varies at the different ports, based on what the rules are.

Ms. MCSALLY. Right.

Ms. GROVER. So, I think we are all in agreement that that is, for the most part, occurring as intended, right? Some room for improvement in the accurate identification of high-risk—

Ms. MCSALLY. But you said previously—

Ms. GROVER. Right. Right, right—

Ms. MCSALLY [continuing]. It was 94 percent missed.

Ms. GROVER. Right. So this is a proxy measure that CBP uses to get a handle on how well does this ATS [Advanced Targeting System] do at identifying high-risk cargo, right? Because they don't really know the true accuracy of that system, because you don't know what you—

Ms. MCSALLY. What you missed.

Ms. GROVER [continuing]. Have missed, right?

Ms. MCSALLY. Right.

Ms. GROVER. Because 99 percent of the shipments—

Ms. MCSALLY. Right.

Ms. GROVER [continuing]. Are determined to be low or medium risk, and generally speaking, moving on through. So we don't actually know what we have missed.

Ms. MCSALLY. So did I misunderstand—

Ms. GROVER. But—

Ms. MCSALLY [continuing]. That 6 percent and 94 percent?

Ms. GROVER. So—well, of the containers that are unpacked, right, of the shipments that are actually subject to physical exam, some number of those have contraband. And CBP keeps records of that. And then they go back and they look and they say, OK, this shipment was unpacked for whatever reason, because it was high-

risk or random or for some other reason. Of the ones that we actually looked at, how many had contraband? And then let's go back to the original designation and say was it originally designated as high risk by the system or not.

And so, yes, for the 9 months or so of data that we looked at in 2011, 2012, the system had only identified 6 percent as high risk. So 94 percent were not. Now, subsequent to that, in the process of responding to our recommendations, the last two quarters of data that I saw were somewhere more in the neighborhood of 25 to 50 percent, which is significantly better.

Ms. MCSALLY. Twenty-five to fifty correctly? There are 50 to 75 percent still missed?

Ms. GROVER. Yes, and that is data from the, you know, roughly late 2014—

Ms. MCSALLY. OK.

Ms. GROVER [continuing]. Time period. So I don't have current data. But, yes, those are the last numbers we—

Ms. MCSALLY. So this is still a problem. If our whole model is based on them identifying high risk, and we are still somewhere in, you know, less than 50 percent being correctly identified, then that is still a problem.

Ms. GROVER. They are still working on it.

Ms. MCSALLY. OK. Mr. Espie, what you shared about not getting access to classified information, you know, port directors not having a sense of what the risks are, we have heard similar things across the private sector in homeland security related to those running sports arenas and other potential targets and vulnerabilities for terrorist attack or terrorist activity. This has been of high interest to me.

So you have no access to fusion centers, no—I just want to make sure we clarify. No access to fusion centers. Would you be interested in having access to fusion centers, you know, classified information briefings for appropriate people at the port? I mean this seems like a gaping hole. We have done better sharing information across Federal agencies, but where we are really missing is Federal down to State and local, and then with the private sector is the real gaping hole.

So, could you just clarify what you would desire, as a solution?

Mr. ESPIE. Thank you, yes. I am fortunate, though. I will note that I do have a secret clearance, and the only reason I do is because I pushed for it through our Baltimore FBI office and through my previous holdings of certain clearances. So I am one of the fortunate ones, probably one of the maybe three or four in the country that have a clearance, in terms of port security directors. So I would look for a model following 9/11 when you saw local police departments at the captain level or so gaining clearances through becoming members of the executive JTTF [Joint Terrorism Task Force] structure within the FBI offices. I would certainly support that.

But overall, even though I have that clearance, I receive nothing. I do not—I am not invited to classified briefings, I do not receive classified information via DHS, Coast Guard. The Bureau, they have just recently offered me to come to classified executive-type

briefings. They are held once a month, so I am going to take advantage of that.

I am confident that if there was information I needed to know, that I would be provided that from our Maryland fusion center. However, I have been here 5 years and have received zero.

Ms. MCSALLY. So, Mr. Chairman, I think this is an area to follow up on. You know, we have been addressing this issue with trying to increase access for the private sector. I think we could probably work together across our committees to maybe work on some initiatives on this.

Thank you, Mr. Chairman. I yield back.

Mr. HUNTER. That is an easy fix. That is a quick, easy fix, fixing that.

Mr. Garamendi, you are recognized.

Mr. GARAMENDI. Chair McSally, you seem to always anticipate my questions. And you were on to one that is very important. I was just thinking as you were asking your question about the recent report that was produced by the French Government on the terrorist attack in France. And the one thing that was most prominent in that report and in other reports is the inability or the lack of sharing of information between the various elements of the safety net, the various police, the intelligence community, and the like. And this is a question that Mr. Espie just raised, and it is one that really needs to have our attention. In all of these situations it comes back to the lack of information being passed on through the various organizations.

Leaving that aside, which does require our continued attention, I want to go to an issue that I know you raised, Mr. Espie, and that is the funding for port security. We heard from the earlier testimony from the Customs and Border Protection that they needed additional funding. I think they talked some 500 personnel. It wasn't clear where they needed to use that. I suspect that—I hope that that is in the ports.

Mr. Espie, can you speak directly to that issue?

Mr. ESPIE. Yes, sir. Two issues. CBP, first of all, at the Port of Baltimore, particularly after the budget concerns a few years ago to whereas it appeared that DHS was negating some of their requests, we have a sense of feel at the Port of Baltimore that CBP is very strapped. In their inspections of cargo within the sheds at our marine terminal, number one, the—we see personnel working the RPMs [radiation portal monitors] during the day, it is a long day. I think they are very bored. I don't think they have enough changeover during the day.

So basically, when these containers leave our ports through going through the RPMs, you are going to have a GS-11 or GS-12, in terms of their morale, motivation, to safeguard a potential nuclear weapon leaving our port and going out to Chicago or the Midwest or—as far as the way we ship.

And also we have had issues at our cruise terminal. We have over 115 cruises through Carnival and Royal Caribbean, through our cruise terminal there. And when there is a shortage, seemingly, when we have—we mandate more power, they advise that they do not have the overtime to pay their officers. So that is a concern. So that is where you see that CBP is going to start potentially

charging port operators for extra services, to include the RPMs. We have been advised that if the RPMs are replaced, that it will be the port operator paying for those and not CBP. So right now we are going through the maintenance phase. So those are concerns.

Secondly, the Federal Port Security Grant Program, we live and die by that. That is our physical security. We would have no physical security at the Port of Baltimore, or at least not in the realm that we have now, which we feel we have one of the most innovative physical security programs in the country. We would be in desperate needs. The State budgeting for that right now, we do—when we receive a match or a grant, it is 25 percent. So the State's ability to cover the physical security necessary is very difficult and short. So we would hope that that program would stay intact.

And also we see—

Mr. GARAMENDI. I am going to interrupt you.

Mr. ESPIE. Yes, sir.

Mr. GARAMENDI. Because I am out of time, literally out of time. I would appreciate it if the—your association, the Port Security Association, could develop a specific memo to us on those kinds of shortcomings, and it is nationally as well as with the Port of Baltimore.

Mr. ESPIE. Yes, sir.

Mr. GARAMENDI. A final point is that the layer—the security through layered operations, beginning way off in Kazakhstan all the way back home, becomes really important. There is a funding issue in each one of these layers, and we really need to get at the funding issues, as well as the efficiency of those particular units along the way.

And so, these kinds of hearings are very, very important, and particularly important that we do the combined hearing that the two chairmen have put together here. That is really an important piece of this, so that we are—at least we are coordinated and knowledgeable with what we are doing here. I want to really focus—and I will ask a series of questions, if the chairs would allow me to do so, to the various witnesses about specific funding shortfalls and the efficiency of the programs that you are operating.

Final point is, Mr. Canavan, you have been here twice and you have talked about a specific type of detection advice—device.

We had earlier Ms. Harrington from NNSA [National Nuclear Security Administration] here. Now, as far as I know, Los Alamos is part of NNSA. And I am curious, and I will get into it from Ms. Harrington as well as from you, about your device and the applicability of that and the utility of that particular mechanism that you have talked about as a detection mechanism.

So, with that, I yield.

Mr. HUNTER. I thank the gentleman. Mr. Gibbs?

Mr. GIBBS. Thanks, Mr. Chairman. I represent the Great Lakes region, so I want to talk to Mr. Weakley.

Great to see you, Jim. In your testimony you talk about the Great Lakes States, and the two Canadian provinces; if they were an entity in themselves, they would be the third largest economy. So we know how important the Great Lakes is, and all the commerce you move. And I am really concerned.

And my other subcommittee, I am chairman of the Subcommittee on Water Resources and Environment. I have stressed so much with the Army Corps of Engineers about the importance of the Soo lock and the Poe lock, and that is—Poe lock is over 100 years old. And my understanding, they built cofferdams years ago and it is just sitting—seems like there is a reluctance with the administration to want to, you know, build new locks there and replace them.

So there's kind of two questions here, two themes. We have the infrastructure issue, and then we have security of the locks. I want to get both of that. But the first part of that is on the Poe lock or the Soo locks there, if that were to shut down, what happens to the Great Lakes?

Mr. WEAKLEY. Well, sir, according to the DHS report, if the lock, a single lock—the Poe, as you point out—is down for 6 months, North America is in a recession equal to or greater than the one that we just experienced.

And also in a resource-based recession there is no fiscal policy you can do to countermand that. So the closest thing we have experienced as a Nation is the oil embargo from the 1970s. It will wipe out the automobile industry, it will wipe out the domestic steel industry. And really, it is a—it is the most critical piece of infrastructure—

Mr. GIBBS. I think we got the picture. I think during World War II they were so concerned about that I think they had, I don't know—

Mr. WEAKLEY. I think it was 20,000 troops stationed in Michigan—

Mr. GIBBS. 20,000 troops regarding that.

Mr. WEAKLEY. Yes, sir.

Mr. GIBBS. So I have stressed so much on the Army Corps how important this is, and there is this reluctance.

Do you know if there has been any initial cost estimates to do the work there?

Mr. WEAKLEY. So where we are at now is the Corps is engaged in a 2-year economic reevaluation report, basically to recalculate the benefit to cost ratio. To give the Corps credit, they have acknowledged that they made some egregious false assumptions in their latest 2004 report. That was a 10-year process for them to make that admission. And now they are recalculating the ratio. They said they could condense the 3-year process into 2 years, which means in December of 2017 they should be done with their math, which means probably December—

Mr. GIBBS. I told Secretary Darcy in my subcommittee hearing that we could sit down right now and in 15 minutes get a cost estimate benefit ratio. That should be a no-brainer.

Mr. WEAKLEY. Yes, sir.

Mr. GIBBS. There is just a huge reluctance, I think, with the administration to want to move forward on that.

OK. So that is the infrastructure issue. We know what happens. This ought to be a top priority for our national economic security and security in general.

What are your thoughts in the Great Lakes are, in the St. Lawrence and all that, on overall security of our—of those assets? We know if that lock breaks the economic catastrophe it would be to

the country. But are you satisfied with the security arrangements by the Coast Guard, whoever, to make sure that the lock isn't attacked, or any of the locks?

Mr. WEAKLEY. Well, I think they could do more. I know the Coast Guard has a security zone in the area. The Corps owns the facility, so they have got primary responsibility. I was just up there a couple weeks ago. They are executing a new security contract.

They do, to their credit, make a distinction between the American-flag vessels and the foreign vessels that go through. They don't allow the foreign sailors off the ships. We are allowed off our ships to handle lines, and stuff like that. Clearly, they don't have the 20,000 troops that they did in World War II.

I think the Corps is beginning to recognize the criticality of that piece of infrastructure. And from a—I am very excited about what we are doing with our radar to create more of a visibility and provide real actionable material to the—

Mr. GIBBS. And my last question—we are out of time, but are you—your companies that you represent, I think you said 15 of them, I forget how many you represent, working with Customs and Border Protection, the Coast Guard, and all their law enforcement moving this commerce from the Great Lakes, are you satisfied with the relationship? What are your thoughts?

Mr. WEAKLEY. So, as a former Coast Guard officer, I will expose my bias. We work really well with the Coast Guard. I think with CBP it varies from port to port, and actually it varies from cargo to cargo, and sometimes the distance, whether you are within the Federal-recognized port, as well. I think that relationship could be better.

Giving the Coast Guard credit, they are more centralized. So if there is a problem with the Coast Guard, we can go to the district commander. With CBP there is no regional office. So there is a headquarters level and then they are very autonomous at the local level. I think there could be room for improvement along the CBP from the relationship aspect, as well as the ability to execute.

Mr. GIBBS. OK, thank you.

Thank you, Mr. Chairman, I yield back.

Thanks for your service.

Mr. HUNTER. I thank the gentleman. For a minute I thought you were talking about Polacks.

[Laughter.]

Mr. HUNTER. Now I know you weren't. Poe lock.

Mr. GIBBS. You know, I know San Diego is important, but Great Lakes are really important, too.

Mr. HUNTER. Ms. Jackson Lee, you are recognized.

Ms. JACKSON LEE. I thank the chairman and ranking member for their courtesies, and thank the witnesses as well as the witnesses on panel 1. I was delayed because of a markup in the Judiciary Committee, which fell under my subcommittee. But this is an important hearing, and I want to acknowledge panel 1 and thank panel 2 for their testimony.

Let me start by just citing part of the words said by Director Dave Espie in his testimony, that the threat of maritime terrorist smuggling appears to be increasing, possibly in correlation with the flight of Syrian refugees to Europe. And he noted an incident, I

think, that occurred in Baltimore. But I believe that it is clearly an important hearing that we are addressing today in an examination of the maritime nuclear smuggling threat and other port security and smuggling risks in the United States.

I think our challenge, as Members of Congress, is to find the how-to's or how does, but also the solutions to protect the American people. I am particularly interested, of course, as a former ranking member of our Border and Maritime Security Subcommittee, but as well as a Member of Congress that has as part of her jurisdiction one of the major ports of the United States, and that is the Houston port.

I am a strong supporter of the Securing the Cities program, and as well the monies that you all need, Mr. Espie, in doing your job. So let me start off first by saying we will not solve this problem by ignoring the fact that resources are needed, not throwing money away, but fully funding the potential of what our ports and what the Nation faces.

The Securing the Cities program mandated legislation to assist State, local, tribal, and territorial governments in creating and implementing and perfecting existing structures for coordinated and integrated detection and interdiction of nuclear or other radiological materials that are out of regulatory control, and to support a wide matrix to deal with identifying reporting on nuclear and other radioactive materials, provide resources for detection analysis communication, facilitate the establishment of protocol and processes of effectively responding to threats—responding to threats is key—and designating participating jurisdiction from high-risk areas.

Our city has now received \$30 million over a 5-year period, which I am very glad to advocate and secure under the Securing the Cities grant, and just received \$3.5 million. And in his absence I want to thank Dr. Brasure, who was in my district, as we announced this very important step by Houston, creating or working with the DHS Domestic Nuclear Detection Office to build a robust regional nuclear detection capability.

So, I am going to pursue a line of questioning in the time that I have remaining, and let me quickly do so—is to Dr. Canavan, if you can remember my questions, please, I would appreciate it. How accurately can the signature of radiological and nuclear material tell the source of that material? That is very important because we are talking about ships and smuggling.

To Ms. Grover, thank you for your work in the GAO. In your testimony you cite GAO's 2013 report which concluded that CBP had not regularly assessed foreign ports for risk to cargo since 2005. It is my understanding that they have since developed a port risk matrix and priority map to help assess whether changes need to be made to contain a security in each of their ports. Is CBP utilizing this matrix and map to assess CSI [Container Security Initiative] ports? Are there other changes that should be made to ensure the CSI program is functioning as intended? There lies a source of potential nuclear material.

And finally, to Mr. Espie, you are one of the first responders outside of the beltway. All across America you are dealing with port security, formerly with the FBI. Are resources going to local enti-

ties like yourself crucial in making sure that we have the cover, the resources, the detection that needs to be in place for something as particularly indicting, explosive, and, if you will, catastrophic, as a particular or potential nuclear incident by something being smuggled into your port?

I would yield first to Dr. Canavan. Thank you.

Dr. CANAVAN. To me, ma'am?

Ms. JACKSON LEE. I yield first to you, sir, for the question. Did you hear the question that I asked?

Dr. CANAVAN. Well, I thought the question had to do with—

Ms. JACKSON LEE. Let me read your question, sir. How accurately can the signature of radiological and nuclear material tell the source of that material?

Dr. CANAVAN. With radiological material, it is a little bit difficult, because that is just sort of nuclear garbage, and there is lots of it around the world. And you might get lucky, and you might make an attribution, but I find that unlikely.

With nuclear weapons material, attribution is a little bit cleaner—particularly if you intercept it before detonation—because with—particularly with plutonium, the different groups that make plutonium have different preferred ways of doing it, so there might be some intermediate group that got control of it or delivered it, but you have a fighting chance of knowing who made it in the first place.

So, the attribution is kind of all across the spectrum. I would say very little likelihood of attribution on the garbage side, reasonable chance on the plutonium. For uranium, which is a big problem right now, you know, it is just how long you want to spend your centrifuges, your—and they are all derivatives of Urenco's. Some people try to argue that you can do an attribution there on the basis of their details. I kind of doubt it, although that last statement is just my personal guess.

Ms. JACKSON LEE. Not at all, Doctor, thank you. Just one followup. Can the trash that is hardest to detect provide major damage and danger?

Dr. CANAVAN. No, ma'am. I didn't mean to say it couldn't cause damage.

Ms. JACKSON LEE. No, I am just asking.

Dr. CANAVAN. The thing is that the radiological threats, the dirty bombs that we—

Ms. JACKSON LEE. Right.

Dr. CANAVAN [continuing]. We have been working on for quite some time, can cause a lot of economic damage because you can spread them on somebody's street, or throw them in a building, and then that is a real cost problem. But once that happens, people will generally get the heck out of the way, so the loss of life is smaller for that kind of weapon.

I come from a place where we worry a little bit less about radiological insults than other places.

Ms. JACKSON LEE. Yes.

Dr. CANAVAN. When I first went to Los Alamos, I think we had the universe's only known open pit plutonium mine. We dug up the old plutonium residue from the war, moved it out, and covered it with a thick layer of dirt. It took time and effort, but worked well.



So I may have a more casual attitude than others towards dirty bombs. They are a real problem because their materials are more accessible than those for weapons, but they are not as catastrophic—particularly in terms of loss of life. But I have experts here, right?

Ms. JACKSON LEE. Mr. Chairman, thank you for your courtesy. If I can just—thank you, Doctor—if I could just allow both Ms. Grover and Mr. Espie to finish, and I would be happy to yield back.

Ms. Grover, you heard my question?

Ms. GROVER. Yes, your question was about CBP's Container Security Initiative program?

Ms. JACKSON LEE. Yes.

Ms. GROVER. Which is an initiative under which CBP targeters are placed at foreign ports, and it is operating at about 60 ports right now. And so your observation is that in 2013 GAO found that while those ports had initially been selected based on volume and other risk factors that, indeed, the circumstances across the world can change, and we found that CBP had not revisited the risk issues since around 2005.

And so, when GAO went in and looked at the situation, we found that there were—some of the ports participating were not high risk and, in fact, that there were not CBP targeters at other very high-risk ports.

And so, yes, as you noted, CBP has developed a port risk matrix and a map. They plan to update it every year, and to apply that knowledge against the locations of the 60 ports where they are working. And so if they follow through on that, and use it, then they will at least have a good understanding of the extent to which the program was operating at the highest risk ports. But that remains to be seen, going forward, and then to the extent to which they can make adjustments as appropriate.

Ms. JACKSON LEE. So we need to be monitoring that. And are you going to be assessing them again?

Ms. GROVER. We will continue to keep track of their use of that, yes.

Ms. JACKSON LEE. Thank you. Mr. Espie, on your—

Mr. ESPIE. Yes, ma'am. Thank you.

Ms. JACKSON LEE [continuing]. Comments along with resources.

Mr. ESPIE. Regarding funding—yes, ma'am. Regarding funding, of course, at the port we have certain mandates we must follow, the Maritime Transportation Security Act, and then we have Federal mandates that come under the CBP jurisdiction, specifically screening for nuclear smuggling, for example.

Do we have the resources, Port of Baltimore? No. You heard the percentages of the screening that takes place overseas, or once it comes to the port. I am there every day. I watch this. I see a container ship have 8,000 TEUs on it. How many do they screen a day? Twenty-five, thirty, maybe. You line up in a row, they go through the VACIS [Vehicle and Cargo Inspection System] machine, the x-ray machine, and they—while the other ones are put into storage and units and they are shipped out the next couple days. So the only security device you have left is the RPM machine, which in some cases is 10 years old, the quality is a question, and so forth.

The manpower is certainly a question for CBP because, again, you watch the VACIS, the screening operation going on. You have usually two or three CBP personnel there, the rest are at the screening sheds. And then you will have one or two or three at the RPM exits out of the terminal. So it is a great problem for us and CBP, for the State of Maryland, and really, the citizens of the United States.

Ms. JACKSON LEE. On the overall issue, then, resources are needed across—you are talking about your State, but if you are an example, it would mean that it happens elsewhere, as well.

Mr. ESPIE. Yes, ma'am. I am a member of the AAPA Security Committee. It is consistent throughout the United States.

Ms. JACKSON LEE. Thank you. Mr. Chairman, I would like—thank you for your testimony—Mr. Chairman, I would like to ask unanimous consent to put into the record an article by MarEx dated July 6, "U.S. Ports Want More Action on Dirty Bomb Prevention."

Mr. HUNTER. Without objection.

[The article is on pages 116–117.]

Ms. JACKSON LEE. I thank you. I yield back.

Mr. HUNTER. I thank the gentlelady. Well, here is what we are trying to do here. We are trying to shape what we feel is going to be probably the most dangerous thing that we can encounter as a country, which is a nuclear device on American soil. It is worse than someone shooting up a mall, it is—I mean that is catastrophic. We all agree on that. And I think we are on the precipice of a—let's call it nuclear material being ubiquitous, much more than it is now. Once the Iranians start getting more material, once the North Koreans get better at creating more bad stuff, you are going to have nuclear devices, nuclear material, weaponized nuclear material, I think, throughout the entire world.

And I think if we all focus on a lot of different stuff, but nothing that can affect the American people in the country like a nuclear device going off that is possibly attributable to a nation-state or possibly not. We have no retaliation, no way to get back at somebody—nonstate actors, of course—that will easily and happily throw their lives away to kill Americans.

Anyway, that is what we are doing here. That is why Ms. McSally and I are trying to shape this, because we are—I think we are still in a relative safe zone where there is not a lot of material out there, and we know who has it, we know where they have it, we know how to stop it in the furthest reaches of the world before it even gets to the U.S. or gets in the hands of bad actors, right? But I think that is coming to an end. I think we probably have a 5- to 10-year window, and then we need to have something where we check everything, because it only takes once, right?

And with that, thank you all for being here. Thanks for your testimony, thanks for traveling out here. And the hearing is adjourned.

[Whereupon, at 12:32 p.m., the subcommittees were adjourned.]

*Submit for record*

STATEMENT OF  
THE HONORABLE JOHN GARAMENDI  
SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION AND  
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY  
JOINT HEARING ON  
“AN EXAMINATION OF THE MARITIME NUCLEAR SMUGGLING THREAT AND OTHER  
PORT SECURITY AND SMUGGLING RISKS IN THE U.S.”  
JULY 7, 2016

Mr. Chairman, thank you for scheduling a second oversight hearing – this time with our colleagues from the Committee on Homeland Security Subcommittee on Border and Maritime Security – to assess U.S. port security, including the implementation of Federal programs to prevent and deter U.S. domestic ports from becoming conduits for the trafficking of uncontrolled nuclear materials or other illicit contraband into the United States.

We are blessed in the United States to have 95,000 miles of shoreline, over 360 ports, and an enormous Exclusive Economic Zone encompassing 4.5 million square statute miles. No less than 95 percent of the cargo tonnage that moves in and out of the U.S. moves by water.

Additionally, a 2014 study on the National Economic Impact of the U.S. Coastal Port System found the total economic value of U.S. coastal ports in terms of revenue to businesses, personal income and economic output by exporters and importers to be \$4.6 trillion, or roughly 26 percent of the nation's \$17.4 trillion economy in 2014.

If anyone should question whether the U.S. remains a maritime nation, these facts alone should dispel all doubts.

The U.S. economy benefits greatly from global maritime trade. Moreover, the interconnected domestic system of vessels, ports, waterways, marine terminals, intermodal connections, and other transportation and support services move goods and materials off our docks with seamless efficiency and convenience.

Yet this tremendous U.S. transportation asset also presents a multi-faceted security challenge for U.S. security, intelligence and law enforcement personnel.

As we discussed during our last hearing in October, the threat of a nuclear or radiological “dirty bomb” arriving at a U.S. port is a sobering new reality in a world that seems to grow increasingly more unsettled and dangerous with each passing day.

An idea which was virtually unimaginable fifteen years ago is now the primary focus of a coordinated, multi-layered strategy involving multiple Federal agencies, including the United States Coast Guard, that monitors, patrols and protects all U.S. land, air and maritime ports of entry.

It would appear that the Global Nuclear Detection Architecture and numerous other Federal activities implemented to fulfill this strategy are meeting the ever-evolving challenge. We have kept nuclear threats far outside U.S. borders. We have also stepped up our efforts to counter other maritime security risks, such as the trade in illegal drugs or human trafficking.

Yet we must be forever vigilant. For even though the likelihood of a terrorist cell smuggling weapons of mass destruction into the country in shipping containers remains low, any such attack could be potentially catastrophic.

Moreover, we need to remain agile and adaptive if we expect to stay one step ahead of those who seek to do us harm by whatever means possible.

As we take up this issue again, I would like to learn the following from our witnesses:

- Are we adequately questioning, reevaluating and re-calibrating our underlying assumptions to ensure they remain relevant to current maritime threats and circumstances?

- Are we sufficiently tracking and addressing all known threats, whether that threat is nuclear, chemical or biological? Does our strategy focus disproportionately on one risk?
- And, considering that a future terrorist may be “home grown”, are we doing everything we can to track and monitor small vessels that operate in U.S. domestic waters to ensure that they pose little to no risk to the American public?

Thank you, Mr. Chairman; I look forward to hearing from our witnesses on these and other important questions as we continue our important work securing the U.S. maritime frontier.

U. S. Department of  
Homeland Security  
  
United States  
Coast Guard



Commandant  
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE  
Washington, DC 20593-7000  
Staff Symbol: CG-0921  
Phone: (202) 372-4411  
FAX: (202) 372-8300

**TESTIMONY OF  
REAR ADMIRAL LINDA L. FAGAN  
DEPUTY FOR OPERATIONS POLICY & CAPABILITIES**

**ON  
“PREVENTION OF SMUGGLING AT U.S. PORTS”**

**BEFORE THE  
HOUSE SUBCOMMITTEE ON COAST GUARD & MARITIME TRANSPORTATION  
AND THE  
HOUSE SUBCOMMITTEE ON BORDER & MARTIME SECURITY**

**JULY 7, 2016**

**Introduction**

Good morning Mr. Chairman and distinguished Members of the Committee. It is my pleasure to be here today to discuss layered border security and smuggling in U.S. ports.

The U.S. Coast Guard is the world’s premier, multi-mission, maritime service responsible for the safety, security and stewardship of U.S. waters. At all times a military service and branch of the U.S. Armed Forces, a federal law enforcement agency, a regulatory body, a first responder, and a member of the U.S. Intelligence Community, the Coast Guard operates on all seven continents and throughout the homeland, serving a nation whose economic prosperity and national security are inextricably linked to broad maritime interests.

The Coast Guard protects and defends more than 100,000 miles of U.S. coastline and inland waterways, saves thousands of lives per year, and safeguards the world’s largest Exclusive Economic Zone (EEZ), encompassing 4.5 million square miles of ocean. Indeed, the Coast Guard is fully engaged answering the call and balancing a multitude of dynamic maritime risks facing our nation.

The Coast Guard is also in high demand globally. Many nations model their maritime forces after the U.S. Coast Guard to address transnational crime, human smuggling, maritime safety and security, and foreign incursions into their respective waters.

**A Layered Approach**

Securing our maritime borders requires a layered, multi-faceted approach. Because of its unique authorities, capabilities, competencies, and partnerships, the Coast Guard is well positioned to undertake such an approach and meet a broad range of maritime border security requirements.

This layered approach allows the Coast Guard to detect, deter, and counter threats as early and as far from U.S. shores as possible.

### **Countering Threats in the Western Hemisphere**

The Coast Guard, along with U.S. Customs and Border Protection (CBP), plays a pivotal role in securing our nation's maritime domain. Persistent threats include illegal migration, human trafficking and illicit flows of drugs. The prevalence of Transnational Organized Crime (TOC) networks exacerbates these threats. TOC networks are driven by immense profits from drug trafficking and other illicit activity, and their indiscriminate use of violence weakens regional governments in Central America, stymies legitimate economic activity and development, terrorizes peaceful citizens, and fuels migrant flows.

Coverage by Coast Guard assets in the maritime approaches pays significant dividends by employing timely intelligence from an expanding network of partners. The Service's new National Security Cutters (NSCs), Fast Response Cutters (FRCs) and our legacy cutter and aircraft fleets achieved impressive operational successes in Fiscal Year 2015, and are on track to surpass these successes in Fiscal Year 2016. Critical acquisitions like the Offshore Patrol Cutter (OPC), a more capable and reliable replacement for our outdated Medium Endurance Cutters (MEC), are essential to our long-term success.

In Fiscal Year 2015, the Coast Guard worked with interagency partners to help remove 191.8 metric tons of cocaine and detain over 700 smugglers for prosecution; 144 metric tons and 500 smugglers were removed by Coast Guard assets alone. We also repatriated 2,700 Cuban and 425 Haitian migrants; we continue to closely monitor maritime migration patterns as our relationship with Cuba continues to evolve. Thus far in Fiscal Year 2016, three NSCs alone have made over 25 drug interdictions in the Eastern Pacific, including two cases involving Self-Propelled Semi-Submersible vessels, stopping 28 metric tons of cocaine from reaching our streets. In fact, the Coast Guard is on track to have a record breaking year for drug removals, having already nearly eclipsed Fiscal Year 2015 numbers.

### **International Partnerships**

The Coast Guard's success in maritime border security relies on robust joint, interagency, and international partnerships to conduct operations throughout the Western Hemisphere. To more effectively counter maritime threats in the offshore region and throughout the Western Hemisphere, the Coast Guard maintains more than 40 maritime bilateral law enforcement agreements and arrangements with partner nations. These agreements and arrangements facilitate coordination of operations and the forward deployment of boats, cutters, aircraft, and personnel to deter and counter threats as close to their origin as possible, and enable real time communications between Coast Guard and partner nation operations centers.

To foster international cooperation and build partner capacity, Coast Guard personnel are posted at several embassies throughout the world. These individuals develop strategic relationships with partner nation maritime forces that facilitate real-time operations coordination, maritime security cooperation, confirmation of vessel registry, waivers of jurisdiction, repatriation of undocumented migrants, and disposition of seized vessels, contraband, and detained crews.



Equally important, they provide subject matter expertise and advice for Country Teams to assist U.S. Ambassadors in carrying out comprehensive and coherent U.S. Government foreign policy, and in addressing maritime threats at their source.

#### **International Port Assessments and Vessel Screening**

The Coast Guard conducts foreign port assessments and leverages the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to assess effectiveness of security and antiterrorism measures in foreign ports. Through the ISPS Program, the Coast Guard performs overseas port assessments to determine the effectiveness of security and antiterrorism measures exhibited by foreign trading partners.

Since the inception of ISPS in 2004, Coast Guard personnel have visited more than 150 countries and approximately 1,200 port facilities. These countries generally receive biennial assessments to verify compliance with the ISPS Code and U.S. maritime security regulations, as appropriate. Vessels arriving in foreign ports that are not compliant with ISPS Code standards are required to take additional security precautions while in those ports. They may also be boarded by the Coast Guard before being allowed entry to U.S. ports, and in some cases may be refused entry to the United States. In FY15, the ISPS Program assessed the effectiveness of anti-terrorism measures in nearly 200 port facilities of 60 of our maritime trading partners, as well as conducted 25 capacity building activities in 23 countries with marginal port security to prevent them from falling into non-compliance with the ISPS Code.

In U.S. ports, the Coast Guard Captain of the Port (COTP) is designated as the Federal Maritime Security Coordinator (FMSC). In this role, COTPs lead the nation's 43 Area Maritime Security Committees (AMSCs) and oversee the development, regular review, and annual exercise of their respective Area Maritime Security Plans. AMSCs assist and advise the FMSC in the development, review, and implementation of a coordination and communication framework to identify risks and vulnerabilities in and around ports. Additionally, AMSCs coordinate resources to prevent, protect against, respond to, and recover from Transportation Security Incidents. AMSCs have developed strong working partnerships between all levels of government and private industry stakeholders. The Coast Guard screens ships, crews, and passengers for all vessels required to submit an Advance Notice of Arrival (ANOVA) prior to entering a U.S. port.

#### **Weapons of Mass Destruction (WMD) Detection and Interdiction**

The evolution and proliferation of advanced commercial, military, and dual-use technology, combined with increased availability and sophistication of transportation and delivery systems, creates new opportunities for transnational and domestic terrorist groups to employ WMD to conduct catastrophic attacks against the United States. The Coast Guard, in coordination with joint, interagency, and international partners, prepares for a range of contingencies that would accompany a WMD threat or event. Coast Guard forces contribute to a layered defense around the homeland. They help provide early detection of a WMD threat in the maritime domain, and assist response to maritime terrorist events that may involve a WMD threat aboard a vessel approaching the United States. Coast Guard's major cutters are designed to protect on-board personnel from the chemical, biological, radiological, and nuclear (CBRN) materials and agents and conduct critical post-attack operations in a CBRN environment.

The Coast Guard conducts over 400 routine inspections and general law enforcement boardings every day to ensure that vessels comply with international maritime law and safety standards, applicable U.S. law and regulations, and any control procedures required to access the Nation's ports. Every Coast Guard member who visits a boat, vessel, or regulated facility carries a basic detection device designed to alert the user to the presence of radiation.

In 2004, the Coast Guard developed and implemented a Coast Guard-wide Maritime Radiation Detection program and has since maintained a close relationship with Domestic Nuclear Detection Office (DNDO) to standardize equipment. The Coast Guard participates in DNDO strategic joint radiation detection acquisition programs that seek to standardize or increase compatibility of radiation detection platforms among the key components, including the Coast Guard, CBP, and the Transportation Security Administration (TSA). The Coast Guard also participates in inter-component training sponsored by DNDO. The result of joint acquisitions and training is robust, ongoing Coast Guard support to CBP seaport inspections as well as to TSA Visible Intermodal Prevention and Response (VIPR) Teams at major intermodal and passenger ports.

All operational units - such as Sectors, Deployable Specialized Forces, Cutters, and Boat Stations - possess radiological detection capabilities that can identify specific isotopes, distinguish between man-made and natural sources, and can "reach back" to interagency experts for technical assistance. Additionally, Coast Guard Deployable Specialized forces are equipped to survive and carry out limited operations in a chemical, biological, radiological, or nuclear-contaminated environment.

Coast Guard Maritime Security Response Team (MSRT), located in Chesapeake, VA provide the nation with specialized maritime capability for nuclear and radiological detection and identification, in either routine or hostile situations. MSRT is trained and equipped to interdict, board, and control a vessel of interest either known or suspected of posing a terrorist threat to the United States out to 200 nautical miles from either U.S. coast. MSRT capabilities are specifically designed to integrate with other interagency and DOD response forces.

### **Conclusion**

The Coast Guard's layered maritime border security strategy addresses the broad range of offshore and coastal threats that have the potential to impact our national security and economic prosperity. From efforts to strengthen international and domestic partnerships, to investments in cutter, boat and aircraft recapitalization, the Coast Guard continues to improve maritime border security while facilitating the safe flow of legitimate commerce.

Thank you for the opportunity to testify today, and thank you for your continued support of the U.S. Coast Guard. I would be pleased to answer your questions.

**“Prevention of Smuggling at United States Ports”  
Before the House Transportation & Infrastructure, Coast Guard and Maritime  
Transportation Subcommittee & the House Homeland Security Committee, Border and  
Maritime Security Subcommittee**

**Introduction**

Good morning Chairman Hunter, Chairwoman McSally, Ranking Member Garamendi, Ranking Member Vela, and distinguished Members of the Subcommittees. Thank you for the opportunity to testify with my colleagues from the Department of Homeland Security (DHS) and the Department of Energy (DOE) and for your interest in the Domestic Nuclear Detection Office’s (DNDO) efforts to prevent the smuggling of nuclear or other radioactive materials via our Nation’s maritime ports.

In his opening remarks at the Nuclear Security Summit this past April, President Obama stated that “the danger of a terrorist group obtaining and using a nuclear weapon is one of the greatest threats to global security.” We know that terrorist organizations have long sought nuclear materials, and if given the means, would likely exploit the opportunity to use them for nefarious purposes. While the likelihood of a nuclear attack is presumed to be low, we cannot dismiss the threat itself. An attack on U.S. territory with a nuclear device – or even a radiological dispersal device – would have profound and catastrophic consequences.

The nuclear security enterprise encompasses a spectrum that spans non-proliferation of materials, physical protection of nuclear and other radioactive materials, detection of such materials out of regulatory control, rendering devices safe, response and recovery to incidents, and forensics and attribution of materials and devices. DNDO has specific, focused responsibilities for two elements in this spectrum: nuclear detection and technical nuclear forensics.

To fulfill this mission, DNDO relies upon our partnerships with federal, state, local, tribal, territorial, and international partners as well as those in the private sector, academia, and the national laboratories.

My testimony today focuses on efforts to strengthen the maritime portion of the global nuclear detection architecture, by promoting national nuclear detection architectures abroad, supporting operational readiness domestically, and improving the technical nuclear forensics capabilities of the U.S. government (USG).

**Developing the Global Nuclear Detection Architecture**

DNDO is responsible for the coordination of federal efforts to detect and protect against attempts to import, possess, store, develop, or transport nuclear or other radioactive materials out of regulatory control that may be used as weapons against the Nation.

To that end, DNDO, with its interagency partners from the Departments of Defense (DoD), Energy, State (DoS), Justice (DOJ), and the Office of the Director of National Intelligence (ODNI), coordinates the development and enhancement of the global nuclear detection

architecture, which is a framework for detecting, analyzing, and reporting on nuclear and other radioactive materials that are out of regulatory control. The architecture presents a layered, multi-faceted, defense-in-depth approach to ensure prospective terrorists face multiple obstacles. It serves as the groundwork for continuously improving the Nation's capabilities to detect nuclear or radiological threats internationally and domestically. Further, DNDO is responsible for implementing the domestic portion of the global nuclear detection architecture.

### **International Efforts**

Consistent with our layered approach to detection, DNDO's efforts to secure the homeland from the threat of nuclear terrorism begin overseas. A *global* nuclear detection architecture The exterior layer relies largely on the decisions of sovereign foreign partners to develop and enhance their own national and regional detection architectures. To that end, DNDO promotes the development of national nuclear detection architectures, in close cooperation with the Department of State and other interagency partners and multilateral organizations like the International Atomic Energy Agency (IAEA), the Global Initiative to Combat Nuclear Terrorism (GICNT), and INTERPOL.

Close interagency cooperation is exemplified by DNDO's work with Department of Energy's Office of Nuclear Smuggling Detection and Deterrence (NSDD) for capacity building in the international layer of the global nuclear detection architecture. In addition to NSDD deployments of radiation detection, DNDO-NSDD coordination extends through many enhancement activities, including technical analyses, training, exercises, and other performance evaluations. Both organizations continue to share their collective operational best practices with partner countries to strengthen the global nuclear detection architecture.

Through these same international organizations, DNDO assists partner nations in their endeavors to develop national and regional detection architectures, by promoting guidance, sharing best practices, and offering training courses. These efforts focus on helping nations form the foundational elements of any viable architecture, to include capability in planning, risk assessment, strategy development, legal and regulatory frameworks, and the integration of intelligence networks and law enforcement. To date, DNDO's international outreach and coordination efforts have supported the planning of national-level detection architectures in 84 IAEA Member States.

DNDO also supports broader national outreach efforts designed to support the global nuclear detection architecture. One mechanism of particular benefit has been the Nuclear Security Summits, launched by President Obama in 2010. This series has served as an invaluable international forum for improving global nuclear security within a number of commercial pathways, to include the maritime supply chain. In November 2015, DHS, DOE, and other USG representatives participated in the Nuclear Security Summit Maritime Security Workshop co-sponsored by the United States and the United Kingdom to promote radiation detection in the maritime environment. In total, 15 countries, nine international organizations, three terminal operators, and several academic institutions came together to share best practices and enhance measures to remove materials out of regulatory control. This effort directly supported the

Department's Congressionally-mandated endeavor to scan 100% of U.S.-bound maritime cargo containers overseas.

At the 2016 Nuclear Security Summit, 14 nations endorsed the results and best practices from the workshop. Moreover, 23 countries, along with INTERPOL, recorded their support for a "gift basket"<sup>1</sup> on National Nuclear Detection Architectures, thereby affirming their commitment to strengthening detection capabilities overseas.

In sum, international cooperation and the work accomplished through the Nuclear Security Summit process have provided meaningful contributions to building a multi-faceted, multi-layered approach for detection so nuclear and other radioactive material out of regulatory control can be interdicted before being transported to the United States.

### **U.S. Borders**

The layered approach to countering nuclear terrorism continues at our borders. To fulfill DNDO's responsibility to implement the domestic portion of the global nuclear detection architecture, we work with DHS operational components to develop and deploy detection technologies. DNDO procures large-scale fixed radiation detection systems and small mobile devices for employment at our ports of entry, along our land and maritime borders, and in the interior of the United States. As such, we collaborate with the U.S. Coast Guard (USCG), U.S. Customs & Border Protection (CBP), and the Transportation Security Administration (TSA).

To bolster detection capabilities at our maritime borders, DNDO has procured portable radiation detectors for CBP Air and Marine Operations (AMO) as well as USCG so that all boarding teams are equipped with mobile devices to scan for the presence of radiation. To augment USCG's ability to identify a radionuclide that has been detected, DNDO recently procured a new technology, called Human Portable Tripwire. These small, wearable devices enable faster detection, identification, and adjudication of nuclear and other radioactive sources.

DNDO has also acquired Small Vessel Standoff Detection portable nuclear detection equipment for use by USCG and CBP AMO to increase the probability of detecting threats on-board small vessels when encountering such vessels. To facilitate the scanning of inbound cargo containers, DNDO, in collaboration with CBP, has also procured and deployed radiation portal monitors and radioisotope identification devices for use at the ports of entry. As a result, today, nearly 100% of all incoming maritime containerized cargo is scanned for radiological and nuclear threats at our seaports.

### **Domestic Efforts**

Our layered approach persists within our borders and shores. Building operational detection capacity through training, exercises, and cross-jurisdictional protocols is integral to securing the maritime domain. Therefore, DNDO works with federal, state, local, tribal, and territorial agencies to build flexible, multi-layered capabilities.

---

<sup>1</sup> Gift baskets are nuclear security commitments made jointly by multiple international partners.

To further our domestic capabilities to detect and interdict nuclear and other radioactive material out of regulatory control, DNDO is currently engaged with all 50 states and 36 of the USCG's Area Maritime Security Committees. Since intelligence and information sharing is integral for our collective success, DNDO efforts are focused on bringing together federal, state, local, tribal, and territorial partners at the outset. DNDO and DHS's Office of Intelligence & Analysis, along with our federal interagency partners at the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC), ensure that state and local partners have the information and tools necessary to address evolving threats. State and major urban area fusion centers, State Emergency Control Centers, and the FBI Joint Terrorism Task Forces (JTTFs) provide the necessary information exchange pathways. In the event of an emergency, this connected system provides federal, state, local, tribal, and territorial personnel with the ability to exchange sensitive information in a timely and secure manner.

To enhance situational awareness of radiological and nuclear threats and provide technical support to operational partners, DNDO's Joint Analysis Center provides information products and technical expertise. DNDO's Joint Analysis Center Collaborative Information System provides nuclear alarm adjudication support to operational partners, including state, local, tribal, and territorial partners in the maritime environment. This system is connected to the Triage system, maintained by the DOE's National Nuclear Security Administration, which enables seamless transition when national-level adjudication assistance is required.

DNDO provides program assistance to aid maritime partners in developing radiological and nuclear detection programs based on lessons learned in the West Coast Maritime Pilot, a collaborative effort with partners from Puget Sound, WA, and the Port of San Diego, CA. For example, DNDO has recently been working with the USCG Sector Hampton Roads, a region that includes the entire coast of Virginia, the Chesapeake Bay, and the James River up to the Port of Richmond. DNDO has worked with the region to develop a detection program consisting of a regional concept of operations, standard operating procedures, and multi-year training and exercise plan. Since the establishment of this program, DNDO has assisted the region with several related maritime exercises to ensure operational proficiency and agencies within the region assisted in piloting a newly developed Maritime Radiological and Nuclear Boat Operations course.

To ensure operational partners, including those in the maritime environment, are prepared to respond to a threat, DNDO dispatches a unique "red team" to challenge fielded capabilities using specialized nuclear and other radioactive sources and scenarios. DNDO supports maritime partners by conducting overt and covert assessments of operations by intentionally introducing radioactive sources and mock devices against deployed defenses to evaluate the performance of fielded technology, training, and protocols. Engagements are conducted through the Area Maritime Security Committees or directly with the federal, state, or local maritime agency. Recent engagements included partners from Hampton Roads, VA; San Diego, CA; and Philadelphia, PA.

### Improving Technology

In parallel with efforts to deploy technologies to the field, we continue to explore ways to enhance our fielded capabilities. To improve the performance of radiation portal monitors and gain efficiency at land and maritime ports of entry, CBP and DNDO worked closely on implementing an approach to reduce the number of nuisance alarms. Radiation portal monitors routinely detect benign radioactive materials in the stream of commerce, resulting in a significant operational burden for CBP field officers who must resolve these alarms. CBP and DNDO worked closely to evaluate and implement revised radiation portal monitor parameter settings, reducing nuisance alarms (by 78% on average) without sacrificing detector performance against threat materials. We are also collaborating with CBP's Laboratories and Scientific Services to use machine learning to further reduce the number of nuisance alarms in radiation portal monitors deployed to ports. This algorithm is undergoing an assessment this June-August during which it will be installed and run in the real operational environment on incoming and test cargo as well as a variety of threat and benign sources.

To advance technology to detect threats in the maritime domain, DNDO performs accelerated development, characterization, and demonstration of leading-edge technologies. Two examples of this research and development work include:

- The *Advanced Technology Demonstration* Program, which seeks to bring together advanced detector hardware and smart algorithms for demonstration and characterization. One project is characterizing the Airborne Radiological Enhanced-sensor System, a prototype radiation detection system mounted on a helicopter for aerial searches. This effort seeks to provide a capability via an aircraft-borne detection system during intelligence-driven operations to detect and intercept nuclear and other radioactive threats at distances far removed from major population centers and critical infrastructure, and with faster response times than interdictions made via boats and cutters.
- The *Nuclear and Radiological Imaging Platform* Program, where DNDO is developing and evaluating emerging technologies to detect shielded materials while clearing benign conveyances at land and maritime ports. One such effort is a project with the Massachusetts Port Authority, DHS Science and Technology's Border and Maritime Security Division, and the United Kingdom Home Office to develop and evaluate the next generation non-intrusive inspection imaging equipment. The technology will be evaluated in the Port of Boston next year and, if successful, will demonstrate a next generation integrated system capable of detecting both nuclear material and contraband.

### Advancing Technical Nuclear Forensics

An act of nuclear terrorism or the interdiction of a nuclear or radiological threat at a U.S. port would necessitate rapid, accurate attribution based on sound scientific evidence. Technical nuclear forensics, when coupled with intelligence and law enforcement information, supports leadership in determining the origin of materials and, thereby, facilitators of terrorist activities. DNDO's National Technical Nuclear Forensics Center helps to ensure the readiness of the overarching USG nuclear forensic capabilities, advances our technical capabilities to perform

forensic analyses on nuclear and other radioactive materials seized prior to detonation, and maintains an expertise pipeline for nuclear forensic scientists. As with its detection mission, DNDO must closely collaborate with interagency partners, particularly those in the FBI, DOE, DoD, DoS, and the intelligence community.

The readiness of U.S. nuclear forensics capabilities to respond to events has improved markedly in recent years. This improvement has been demonstrated by the successful execution of increasingly realistic and complex interagency exercises of nuclear forensics operations involving interdicted materials and devices, and post-nuclear detonation scenarios. For example, this past fall, DNDO served as the Lead Planner in a successful land-based and maritime exercise of the National Technical Nuclear Forensics Ground Collections Task Force, whose mission is to collect vital forensic evidence in the immediate aftermath of a nuclear detonation to assist in determining the responsible entity. The task force, comprised of members from the DoD, DOE, and the FBI, collects debris samples near the site of the detonation for analysis at designated laboratories. Exercise Prominent Hunt 15-2, which took place in Southern California, simulated a nuclear detonation near the ocean. This was the first time the task force had to coordinate the collection of simulated forensic evidence at sea.

#### **Closing**

Maritime and port security is vital to the flow of global trade and commerce. An act of nuclear terrorism via our Nation's maritime environment would have potentially catastrophic effects on the global supply chain, both directly and indirectly. To prevent nuclear terrorism, DNDO works collectively with international, federal, state, local, tribal, and territorial partners to enhance capabilities to ensure adversaries encounter multiple obstacles should they seek to attack us using nuclear or other radioactive material. Efforts to develop national and regional detection architectures abroad, research and development to advance technologies for detection, and deployment of systems at and within our borders are imperative to minimize the risk of an attack in the United States. Likewise, our work to continue advancing our national nuclear forensics capabilities is important in ensuring those responsible are held accountable for their actions. We will continue to work with our partners to bolster defenses against the threat of nuclear terrorism, and we sincerely appreciate the attention and support from your subcommittees in preventing such an event from occurring.

Thank you again for this opportunity, and I am happy to answer any questions.





---

TESTIMONY OF

TODD C. OWEN  
Executive Assistant Commissioner  
Office of Field Operations  
  
U.S. Customs and Border Protection  
Department of Homeland Security

BEFORE

U.S. House of Representatives  
Committee on Transportation and Infrastructure  
Subcommittee on Coast Guard and Maritime Transportation  
  
Committee on Homeland Security  
Subcommittee on Border and Maritime Security

ON

"An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security and  
Smuggling Risks in the U.S."

July 7, 2016  
Washington, D.C.

Chairwoman McSally, Chairman Hunter, Ranking Members Vela and Garamendi, and distinguished Members of the Subcommittees, it is an honor to appear before you today to discuss the role of U.S. Customs and Border Protection (CBP) in maritime cargo security, a role that we share with the Department of Homeland Security (DHS) agencies that join me today.

As the lead DHS agency for border security, CBP works closely with our domestic and international partners to protect the Nation from a variety of dynamic threats, including those posed by containerized cargo and commercial conveyances arriving at our air, land, and sea ports of entry (POE). CBP's security and trade facilitation missions are mutually supportive: by utilizing a risk-based strategy and multilayered security approach, CBP can focus time and resources on those suspect shipments that are high-risk which, in turn, allows CBP to expedite legitimate trade. This approach incorporates three layered elements to improve supply chain integrity, promote economic viability, and increase resilience across the entire global supply chain system:

- *Advance Information and Targeting.* Obtaining information about cargo, vessels, and persons involved early in the shipment process and using advanced targeting techniques to increase domain awareness and assess the risk of all components and factors in the supply chain;
- *Government and Private Sector Collaboration.* Enhancing our Federal and private sector partnerships and collaborating with foreign governments to extend enforcement efforts outward to points earlier in the supply chain; and
- *Advanced Detection Equipment and Technology.* Maintaining robust inspection regimes at our POEs, including the use of non-intrusive inspection equipment and radiation detection technologies.

These interrelated elements are part of a comprehensive cargo security strategy that enables CBP to identify and address the potential use of containerized cargo to transport radiological weapons, such as "dirty bombs," radiological dispersal devices (RDD), or other dangerous materials, before they arrive at our Nation's border.

#### **Advance Information and Targeting Capabilities**

CBP's multilayered approach to cargo security necessitates substantial domain awareness and intelligence to effectively identify and address high-risk shipments. Statutory and regulatory requirements for the submission of advance information, and the development of rigorous targeting capabilities at the National Targeting Center (NTC), enable CBP to detect potential threats before a vessel or shipment arrives.

The Trade Act of 2002,<sup>1</sup> which provides statutory support for our 24-Hour Advance Cargo Manifest rule, requires importers and carriers to submit to CBP advance electronic cargo information for all inbound shipments in all modes of transportation. Furthermore, CBP requires

---

<sup>1</sup> Pub. L. No. 107-210

the electronic transmission of additional data, as mandated by the Security and Accountability for Every Port (SAFE Port) Act of 2006,<sup>2</sup> through the Importer Security Filing and Additional Carrier Requirements rule (also known as “10+2”). This advance information requirement is a critical element of CBP’s targeting efforts at the NTC and enhances CBP’s capability to identify high-risk cargo without hindering legitimate trade and commerce.

The NTC, established in 2001, coordinates and supports CBP’s anti-terrorism activities related to the movement of cargo in all modes of transportation – sea, truck, rail, and air. Using the Automated Targeting System (ATS), NTC proactively analyzes advance cargo information before shipments depart foreign ports. ATS incorporates the latest cargo threat intelligence and national targeting rule sets to generate a uniform review of cargo shipments, and provides comprehensive data for the identification of high-risk shipments. ATS is a critical decision support tool for CBP officers working at the NTC, the Advanced Targeting Units at our POEs, and foreign ports abroad.

#### **Collaboration with Government and Private Sector Partners**

CBP’s advanced targeting capabilities are further strengthened by our extensive partnerships with other agencies, both domestically and abroad. We work closely with our DHS partners, including the U.S. Coast Guard, U.S. Immigration and Customs Enforcement (ICE), and the Science and Technology Directorate (S&T) to coordinate cargo security operations and deploy advanced detection technology. Furthermore, in 2011, the CBP Commissioner, USCG Commandant and ICE Director signed the cross-component Maritime Operations Coordination (MOC) plan. The plan addresses the unique nature of the maritime environment and sets forth a layered, DHS-wide approach to homeland security issues within the maritime domain, ensuring integrated planning, information sharing, and increased response capability in each area of responsibility. CBP also collaborates with the Domestic Nuclear Detection Office (DNDO) as well as with numerous agencies within the Departments of Defense, Energy, Health and Human Services, Commerce, Justice, and Treasury to promote real-time information sharing.

CBP has participated in numerous joint-operations that led to the interdiction of illicit shipments. For example, Project Zero Latitude was developed due to escalation of foreign and domestic narcotics interceptions involving sea containers of produce and seafood shipments, particularly involving Ecuador. At the NTC, CBP conducted an analysis of historical ATS information and cocaine seizure data. The analysis enabled NTC to identify several smuggling trends that will facilitate the identification of future suspect shipments.

Close collaboration with our Federal partners increases information sharing, which, in turn, enhances CBP’s domain awareness, targeting capabilities, and ability to intercept threats at, or approaching, our borders. CBP continues to extend our cargo security efforts outward through strategic partnerships with foreign countries through the development of international cargo security programs and initiatives.

---

<sup>2</sup> Pub. L. No. 109-347

### *International Partnerships*

One of CBP's most effective international cargo security programs is the Container Security Initiative (CSI). This initiative was established in 2002 with the sole purpose of preventing the use of maritime containerized cargo to transport a weapon of mass effect (WME)/weapon of mass destruction (WMD) by ensuring all containers identified as potential risks for terrorism are inspected at foreign ports before they are placed on vessels destined for the United States. Through CSI, CBP officers stationed at CSI ports abroad and the NTC in Virginia work with host countries' customs administrations to identify and mitigate containers that may pose a potential risk for terrorism based on advance information and strategic intelligence. Those administrations use a variety of means, including detailed data assessment, non-intrusive inspection (NI), radiation detection technology, and/or physical examinations to screen the identified high-risk containers before they depart the foreign port.

CBP works closely with host country counterparts to build their capacity and capability to target and inspect high-risk cargo. Today, in addition to weapons-detection, many CSI ports are now also targeting other illicit materials, including narcotics, pre-cursor chemicals, dual-use technology, stolen vehicles, weapons and ammunition, and counterfeit products. Furthermore, advancements in technology have enabled CBP to increase the efficiency of CSI operations without diminishing effectiveness by conducting more targeting remotely at the NTC. CBP's 60 CSI ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America currently prescreen over 80 percent of all maritime containerized cargo that is imported into the United States. We anticipate that percentage to increase in the near future. Under a revised Declaration of Principles signed on June 23, 2015, CBP and the General Administration of Customs of the People's Republic of China have agreed to expand cooperation to address all cargo hazards, increase information sharing and collaboration, and conduct joint inspections in additional ports in China.

CBP's strong working relationship with our foreign partners is also exemplified by the Secure Freight Initiative (SFI) in Qasim, Pakistan. Through SFI-Qasim, 100 percent of containerized maritime cargo is scanned (by both radiation detection and imaging equipment) prior to lading onboard a U.S.-bound vessel. All targeting of containers and monitoring of the scanning is done remotely via live video feed by CBP officers working at the NTC. Physical examinations are conducted at Port Qasim by Pakistani Customs officials and Locally Engaged Staff hired and vetted by the U.S. Consulate General in Karachi. These physical examinations are also monitored by live-feed at the NTC.

Creating the process for real-time data transmission and analysis in Qasim required the development, installation and integration of new software and equipment. CBP partnered with the Department of Energy to deploy networks of radiation detection and imaging equipment in Qasim. Port Qasim continues to showcase the SFI program in a country where the government and terminal operators support the initiative, and where construction of dedicated facilities is possible. From constructing the scanning site to providing adequate staffing levels for SFI, the Government of Pakistan remains a strong partner in deploying SFI operations.

In addition to Port Qasim, Pakistan, CBP is now also scanning 100 percent of all U.S.-bound cargo containers from the Port of Aqaba, Jordan, using trained and vetted foreign-service

nationals. In July 2016, the Port of Aqaba will be fully functional and able to transmit scan data in real-time to the NTC. Similar to implementing operations in Qasim, CBP received the full support of the Government of Jordan to implement 100 percent scanning in Aqaba. In addition to that support, successful implementation of 100 percent scanning was possible due to the low to medium volume of U.S.-bound cargo processed through the port, and the small percentage of transshipped cargo, which allowed scanning equipment to be placed at the entrance to the port so as not to hinder the flow of cargo movement.

The impact of these programs has been amplified by the close collaboration between CBP and Department of Energy's Office of Nuclear Smuggling Detection and Deterrence (NSDD). Many CSI ports integrate into their operations partner country radiation detection equipment deployed by NSDD. In a similar fashion, CBP and NSDD collaborated in the detection equipment installation at the SFI operations in Qasim. The strong coordination between CBP and NSDD extends to information and resource sharing that enhances the security of maritime supply chain.

All trading nations depend on containerized shipping for the transportation of manufactured goods, which underscores the importance of these two programs. Each year, about 108 million cargo containers are transported through seaports around the world, constituting the most critical component of global trade. Almost 90 percent of the world's manufactured goods move by container, and about 40 percent arrive by ship. Collaboration with foreign counterparts provides increased information sharing and enforcement, further secures the global supply chain, and extends our security efforts outward.

#### *Private-Sector Partnerships*

In addition to CBP's targeting capabilities, and our partnerships with Federal and foreign partners, a critical component to CBP's effort to extend our cargo security to the point of origin is our effective partnership with the private industry. CBP works with the trade community through the Customs Trade Partnership Against Terrorism (C-TPAT) program, which is a public-private partnership program wherein members of the trade community volunteer to adopt tighter security measures throughout their international supply chains in exchange for enhanced trade facilitation, such as expedited processing. C-TPAT membership has rigorous security criteria and requires extensive vetting and on-site visits of domestic and foreign facilities. This program has enabled CBP to leverage private sector resources to enhance supply chain security and integrity.

C-TPAT membership has grown from just seven companies in 2001 to more than 11,000 companies today, accounting for more than 54 percent (by value) of goods imported into the United States. The C-TPAT program continues to expand and evolve as CBP works with foreign partners to establish bi-lateral mutual recognition of respective C-TPAT-like programs. Mutual Recognition as a concept is reflected in the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade, a strategy designed with the support of the United States, which enables Customs Administrations to work together to improve their capabilities to detect high-risk consignments and expedite the movement of legitimate cargo. These arrangements create a unified and sustainable security posture that can assist in securing and facilitating global cargo trade while promoting end-to-end supply chain security. CBP currently has signed Mutual Recognition Arrangements with New Zealand, the European Union,

South Korea, Japan, Jordan, Canada, Taiwan, Israel, Mexico, and Singapore and is continuing to work towards similar recognition with China, Brazil, the Dominican Republic, India and other countries.

#### **Advanced Detection Equipment and Technology**

In addition to deploying technology and personnel abroad under programs like CSI, CBP has made strides in strengthening detection equipment capabilities in domestic seaports. Non-Intrusive Inspection (NII) technology enables CBP to detect materials that pose potential nuclear, radiological, and other materials, such as concealed contraband. Technologies deployed to our Nation's land, sea, and air POEs include large-scale X-ray and Gamma-ray imaging systems, as well as a variety of portable and handheld technologies. NII technologies are force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate cargo. We continue to work closely with S&T to identify and develop technologies to improve our NII capabilities.

CBP currently has 307 large-scale NII systems deployed to, and in between, U.S. POEs. These systems enable CBP officers to examine cargo conveyances such as sea containers, commercial trucks, and rail cars, as well as privately owned vehicles, for the presence of contraband without physically opening or unloading them. This allows CBP to work smarter and faster in detecting contraband and other dangerous materials. As of Sept. 30, 2015, CBP has used the deployed NII systems to conduct more than 81 million examinations, resulting in more than 18,400 narcotics seizures, with a total weight of more than 4.1 million pounds, and more than \$79.2 million in currency seizures.

An integral part of the CBP comprehensive strategy to combat nuclear and radiological terrorism is the scanning of all arriving conveyances and containers with radiation detection equipment prior to release from the POE. In partnership with DND, CBP has deployed nuclear and radiological detection equipment, including Radiation Portal Monitors (RPM), Radiation Isotope Identification Devices (RIID), and Personal Radiation Detectors (PRD) to 328 POEs nationwide.<sup>3</sup> Utilizing RPMs, CBP is able to scan 100 percent of all mail and express consignment mail and parcels; 100 percent of all truck cargo, 100 percent of personally owned vehicles arriving from Canada and Mexico; and nearly 100 percent of all arriving sea-borne containerized cargo for the presence of radiological or nuclear materials. Since the inception of the RPM program in 2002 through May 2016, CBP has scanned more than 1.2 billion conveyances for radiological contraband, resulting in more than 3.9 million alarms, all of which have been successfully adjudicated at the proper level.

When the RPM alarms on a conveyance or package, the conveyance or package is referred to secondary inspection. If it is a conveyance, the driver and all passengers are removed from the vehicle. A RIID is then used to determine if the cause of the radiation alarm is due to an isotope used in medical treatments. Otherwise, using the RPM printout page, the CBP officer will complete a 360 degree scan of the conveyance using a RIID. Once the source of the radiation is

---

<sup>3</sup> As of June 1, 2016, CBP currently has 1,293 RPMs, 2,673 RIIDs, and 33,394 PRDs operational systems deployed nationwide.

localized, the officer uses the RIID to identify the radiation isotope. The results are referred for technical analysis through the CBP Laboratories and Scientific Services Directorate Teleforensic Center.

As part of CBP's NII recapitalization plan, older technology will be phased out and replaced with more modern and state of the art technology. As part of the joint CBP/DNDO RPM Program Executive Plan, older RPMs will be replaced with more capable technology that is more effective and significantly more efficient. CBP's RIID fleet is in the middle of a major recapitalization. Within the last three years, 27 percent of the RIIDs have been replaced with more precise technology. DNDO has also awarded contracts to replace the remainder over next few years subject to the continued availability of funding. DNDO has also awarded a contract for Human Portable Tripwire (HPT) devices for TSA, USCG and CBP – specifically the U.S. Border Patrol (USBP). The device, for USBP operations, is intended to augment their current suite of radiation detection equipment and to help expedite the adjudication of benign radiation alarms, stemming primarily from medical patients traversing through USBP checkpoints. USBP has conducted limited user evaluation of these systems and plans, will deploy an initial quantity in Fiscal Year (FY) 2016, and will derive a wider deployment strategy based on the utility of the system in full operations.

CBP and DNDO continue to collaborate with port and terminal operators to enhance the Department's agility, responsiveness, operational efficiencies, and unwavering commitment to our mutually supporting objectives of safety, security, and prosperity. Two key examples of this are our current project with Port of Los Angeles' Trans Pacific Container Service Corporation (TraPac), LLC Terminal and the Middle Harbor Terminal Redevelopment Project. CBP is currently re-engineering our operations in support of TraPac. TraPac is investing in technology and infrastructure towards an automated terminal that will support both the targeted NII X-ray/gamma-ray imaging of targeted commerce, and the 100 percent mandated radiation scanning<sup>4</sup> of all incoming commodities at the TraPac terminal. CBP, DNDO and TraPac have developed a new and innovative manner for the TraPac Intermodal Container Transfer Facility on-dock rail application utilizing conveyor systems that will transport cargo containers past RPM detector units in fixed positions inside the automation area. This innovative solution will make significant operational improvement to both CBP and TraPac.

The Middle Harbor Terminal Redevelopment Project, sponsored by the Long Beach Container Terminal (LBCT) at the Port of Long Beach, combines two aging shipping terminals into the greenest, most technologically advanced container terminal in the world. With the Panama Canal expansion, the Middle Harbor Terminal will now be able to accommodate super ships, at a maximum of two 18,000 TEU vessels and one 8,000 TEU vessel.<sup>5</sup> The first super ships arrived in Spring 2016, and the terminal is projected to handle 3.3 million TEUs per year by 2019. The terminal will be a state-of-the-art fully automated container terminal, and will utilize automated guided vehicles to move the intermodal cargo containers throughout the terminal, which will streamline CBP's cargo screening processes while allowing them to scan the increased cargo without affecting the flow of trade. In FY 2015, CBP worked with LBCT to develop operational

<sup>4</sup> Security and Accountability For Every Port Act of 2006 (or SAFE Port Act, Pub.L.109-347)

<sup>5</sup> TEU stands for Twenty-Foot Equivalent Unit, which is used to describe a ship's cargo carrying capacity.

requirements, verify concepts of operations, complete an operational assessment, and develop standard operating procedures to support this project. CBP officers will utilize two fixed high-energy large-scale NII systems and RPMs. Officers will no longer utilize the mobile x-ray systems. Additionally, the port has upgraded the optical character recognition system, new road ability islands, transponders for truck identification and a new energy storage building for the automated vehicles.

In conjunction with CBP's many other initiatives (C-TPAT, ATS, NTC, 24-Hour Rule, and CSI), advancements in cargo screening technology provides CBP with a significant capacity to detect illicit nuclear and radiological materials and other contraband and continues to be a cornerstone of CBP's multilayered cargo security strategy.

#### **CBP Small Vessel Programs and Physical Vessel Surveillance**

In addition to the nearly 700 cargo ships that arrive in U.S. POEs daily, the maritime domain supports the commercial fishing industry and its 110,000 fishing vessels, as well as millions of recreational boaters. Most traffic on U.S. waterways and within ports involves legitimate boaters and commercial operators, but it can also involve those engaged in illegal or dangerous activities. A key requirement for enhancing U.S. national security efforts is the ability to identify those who intend to do harm hiding within the sizable majority of people engaged in legitimate activities.

While the *Maritime Transportation Security Act of 2002* (MTSA) and the *International Convention for the Safety of Life at Sea* (SOLAS) require many commercial, passenger, and fishing vessels to operate with an Automatic Identification System (AIS), a tracking system to, among other things, increase maritime awareness, the requirement does not cover many small vessels. The United States Coast Guard (USCG) estimates that, combined with unregistered watercraft, there are approximately 17 million small vessels<sup>6</sup> operating in U.S. waterways; the majority of these vessels is not required to utilize AIS. Therefore, detecting and assessing the risk of small vessels is particularly challenging. We continue to work closely with S&T to identify and develop technologies to improve our small vessel surveillance, detection and tracking capabilities. This includes investments in data integration, information sharing, and land, air and space based sensor systems.

Operators of small pleasure vessels, arriving in the United States from a foreign port or place are required to report their arrival to CBP immediately upon arrival.<sup>7</sup> CBP also requires a face-to-face inspection unless the operator and passengers qualify for an alternate inspection program. In support of the DHS *Small Vessel Security Strategy*,<sup>8</sup> and as part of CBP's comprehensive effort to improve the security of our Nation's borders while enhancing legitimate travel specifically for

<sup>6</sup> "Small vessels" are characterized as any watercraft, regardless of method of propulsion, less than 300 gross tons. Small vessels 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. DHS, *Small Vessel Security Implementation Plan Report to the Public*, January 2001, page 1. <http://www.dhs.gov/xlibrary/assets/dhs-uscg-small-vessel-security-strategy-report-to-public-012011.pdf>.

<sup>7</sup> 19 CFR 4.2

<sup>8</sup> *DHS Small Vessel Security Strategy*, April 2008 (<https://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf>).



small boaters, CBP utilizes several alternate inspection programs such as the Canadian Border Boater permit (I-68), Nexus Marine program, and the Small Vessel Reporting System (SVRS).

SVRS, a voluntary, online program to report the foreign travel of small vessel operators and passengers, was developed to better track small vessels and make it easier to identify suspicious or unknown vessels. Enrollment in SVRS includes completing an online application, attending a face-to-face interview with a CBP officer, and, if needed, providing biometrics for verification. Once enrolled, participants are able to submit a “float plan” consisting of biographical information of all persons intending on traveling, vessel registration information, and itinerary information. By enrolling and submitting a float plan, participants may not have to appear in person for inspection by a CBP officer each time they enter the United States. Participants are still required to report via telephone their arrival in the United States.

In addition to enforcing reporting requirements, CBP uses an array of vessels and aircraft to provide critical aerial and maritime surveillance of known air, land, and maritime smuggling routes to detect, monitor and disrupt illicit activities before they reach the shore. Within the “customs waters”<sup>9</sup> of the United States, or at any place within the United States, CBP Air and Marine Operations (AMO) agents may board a vessel for the purpose of enforcing customs law, and to use all necessary force to compel compliance.<sup>10</sup> Additionally, AMO has jurisdiction over any American vessel on the high seas,<sup>11</sup> and vessels subject to U.S. jurisdiction under the *Maritime Drug Law Enforcement Act*,<sup>12</sup> which concerns the trafficking of controlled substances aboard vessels in extraterritorial waters. These authorities enable AMO to extend the zone of security surrounding our maritime border and littorals of the United States.

In their capacity as CBP law enforcement agents, AMO agents have a critical role in the enforcement of immigration laws in the maritime environment.<sup>13</sup> AMO is uniquely positioned – organizationally, via broad enforcement authorities and jurisdiction, and with unequaled specialized training, equipment, and domain awareness capability – to protect America’s security interests beyond the nation’s border in source and transit zones, between ports of entry, in our coastal waters, and within the nation’s interior. Similar to other investigative agencies, AMO agents recruit confidential sources, develop criminal cases, support prosecutors and testify in court in addition to their enforcement actions in the air, land and maritime domains.

Initiatives such as SVRS, combined with unique air and marine enforcement capabilities, provide CBP with advanced vessel information and increased awareness of small vessels approaching or traveling U.S. waterways. Segregating low risk vessels facilitates legitimate recreational boater traffic and increases CBP’s ability to identify higher risk vessels and dedicate resources to address illicit maritime activities.

---

<sup>9</sup> See 19 U.S. Code § 1401.

<sup>10</sup> See 19 U.S. Code § 1581.

<sup>11</sup> See 19 CFR 162.3.

<sup>12</sup> See Title 46, 46 U.S. Code § 70501-70502.

<sup>13</sup> See Title 8, Aliens and Nationality.

### **Response to a Radiological Weapon at a Port**

The aforementioned technology, targeting capabilities, and partnerships are strategically aligned to prevent the arrival of dangerous weapons, or other dangerous materials, at a U.S. port. However, in the event such a circumstance occurs, CBP has established contingency plans and standard processes in order to ensure a coordinated and effective response to such an event.

Frontline CBP personnel, upon detection of a suspect radioactive source such as a dirty bomb, are trained to secure, isolate, and notify suspect targets and contact the CBP's Teleforensic Center. The scientists are specially trained in spectroscopy to recognize illicit radiological material and can confer with DOE's Triage Program for additional analysis. Any potential threat information will be shared comprehensively and immediately with the FBI Joint Terrorism Task Forces (JTTFs) so that threats can be investigated and resolved. The FBI has the lead for the operational law enforcement response to a domestic terrorist threat or incident. CBP will coordinate with and assist the FBI as part of the response..

CBP's aviation assets maintain an emergency response capability to provide airborne assessment of radiological deposition following a nuclear or radiological accident or incident, and provide airborne detection of a lost or stolen radiological source or device. Under an Interagency Agreement with the DOE National Nuclear Security Administration, CBP provides material, supplies, fuel, aircraft, flight crews, ground crews, and other required resources to provide aircraft flight support for the NNSA radiological emergency response mission.

All frontline personnel working at POEs utilize Personal Radiation Detectors (PRD), and receive ongoing training on how to respond to a detected radiological weapon. A dirty bomb uses common explosives to spread radioactive materials over a targeted area. It is not a nuclear blast. The force of the explosion and radioactive contamination will be more localized. While the blast will be immediately obvious, the presence of radiation will not be known until trained personnel with specialized equipment are on the scene. As with any radiation, frontline personnel are trained to limit the risk and effects of exposure by finding a shielding object, increasing their distance from the blast, and minimizing exposure time. Personnel will also work with local HAZMAT to cordon off a perimeter and assist with the decontamination process.

### **Conclusion**

Each year, more than 11 million maritime containers arrive at our Nation's seaports. At our land borders, another 11 million arrive by truck and 2.7 million by rail. CBP's targeting activities, in conjunction with programs like CSI and C-TPAT, increase CBP's awareness of what is inside those containers, and enhance our capability to assess whether it poses a risk to the American people.

Working with our DHS, Federal, international, state, local, tribal, and private industry partners, CBP's cargo security programs help to safeguard the Nation's borders and ports from threats – including those posed by radiological weapons.

Chairwoman McSally, Chairman Hunter, Ranking Members Vela and Garamendi, and distinguished Members of the Subcommittees, thank you for the opportunity to testify today. I would be pleased to answer your questions.

Statement of Anne Harrington  
Deputy Administrator for Defense Nuclear Nonproliferation  
National Nuclear Security Administration  
U.S. Department of Energy  
on the  
Prevention of Smuggling at U.S. Ports  
Before the  
U.S. House of Representatives  
  
Subcommittee on Border and Maritime Security  
House Committee on Homeland Security  
  
Subcommittee on Coast Guard and Maritime Transportation  
House Committee on Transportation and Infrastructure

July 7, 2016

**I. INTRODUCTION**

Chairwoman McSally, Chairman Hunter, Ranking Member Vela, Ranking Member Garamendi, and distinguished Members of the Subcommittees, thank you for giving me the opportunity to testify on the Department of Energy National Nuclear Security Administration's (DOE/NNSA) efforts to detect, deter, and investigate the illicit smuggling of nuclear and other radioactive materials. Thank you for your continued interest and leadership on this important issue. I would also like to thank my colleagues from the Department of Homeland Security for being constructive and indispensable partners in the effort to reduce the risk of radiological incidents.

NNSA's core mission pillars are to maintain a safe, secure, and effective nuclear deterrent; to prevent, counter, and respond to the threats of nuclear proliferation and terrorism worldwide; and to provide naval nuclear propulsion. The role of NNSA's Office of Defense Nuclear Nonproliferation (DNN) is to prevent non-state actors and proliferant states from developing nuclear weapons or acquiring weapons-useable nuclear material, equipment, technology, and expertise; and to prevent non-state actors from acquiring nuclear and radiological materials for an improvised nuclear device (IND) or radiological dispersal device (RDD). Although technology and expertise are important to anyone attempting to develop a weapon or improvised device, an adversary's ability to access material is essential. Consequently, minimizing the availability of materials, securing them, and interdicting them when they are out of regulatory control are all key elements of our mission. Our programs are organized to reflect this:

- **Material Management and Minimization (M<sup>3</sup>):** Minimize and, when possible, eliminate excess weapons-usable nuclear material, ensure sound management principles for remaining nuclear materials, and support peaceful uses of nuclear energy by making nuclear materials available for these purposes;

- **Global Material Security (GMS):** Achieve adequate security, protection, control, and accounting for all nuclear and radiological materials worldwide (in accordance with internationally accepted recommendations), and prevent the illicit trafficking of nuclear weapons and nuclear and radiological materials;
- **Nonproliferation and Arms Control (NPAC):** Prevent the proliferation of weapons of mass destruction (WMD)—as well as relevant dual-use materials, equipment, technology, and expertise—by state and non-state actors through nuclear safeguards and export controls and by strengthening nonproliferation and arms control regimes;
- **Nonproliferation Research & Development (R&D):** Develop effective technologies to detect nuclear weapons proliferation and nuclear detonations and support monitoring and verification.

Today, I would like to focus my remarks on DNN's efforts to prevent the smuggling of nuclear and radiological materials that could be used in an IND or a RDD. To frame the issue, I would like to take a few moments to describe the threat landscape.

## II. THREAT LANDSCAPE

Securing nuclear and radiological materials from theft, diversion or trafficking is a critical element of U.S. national security strategy. Terrorist groups have sought nuclear and radiological materials and the expertise needed to weaponize them. More than 30 countries currently possess weapons-useable nuclear material stored at hundreds of sites, with the largest inventory in Russia. In addition, radiological materials are ubiquitous, with more than 100 countries possessing radiological material stored at thousands of sites. Despite much progress over the past twenty years by international cooperative programs to improve the security of these materials, gaps remain.

In addition, unknown quantities of material may already be out of regulatory control and the existing black market for nuclear and radiological materials, to include, recent examples of interdictions in countries like Georgia and Moldova, demonstrates this. Beyond the examples of these recent interdictions, Russia's decision to halt most of our nuclear security cooperation leads to a concern that security controls on material in Russia are weakening. Furthermore, the expansion of ungoverned spaces and entrenched corruption in many regions of the world create safe havens for terrorists, compounded by the emergence of an adversarial pseudo-state (self-proclaimed Islamic State of Iraq and Syria) with a demonstrated capability to conduct international terror operations and some expressed interest in acquiring and using radiological and possibly nuclear materials against Western interests.

As you well know, the use of a high-yield IND in a major U.S. city would cause hundreds of thousands of fatalities. The use of an RDD would not cause a large loss of human life, but

would be a destabilizing force and could have global social and economic impacts. Because the threat is so complex and continuously evolving and the physical, economic, and psychological consequences of terrorists using a nuclear or radiological device are so high, significant resources and a multifaceted and layered approach must be employed to counter the threat.

### III. EFFORTS TO PREVENT NUCLEAR SMUGGLING

In this environment, the U.S. Government has developed integrated and enduring strategies to prevent terrorists from obtaining nuclear and radiological materials. Within DNN, much of this work is done by the Office of Global Material Security (GMS), which collaborates with partners within our government and partners worldwide to build sustainable capacity to secure nuclear weapons, weapons-usable nuclear material, and radiological material, and to detect the illicit trafficking of those materials. We have more than 20 years of experience in this area and have worked with over 100 countries. We employ a robust sustainability approach that focuses on gradual transition of responsibility to the partner and continued engagement once a partner assumes responsibility for an activity. We also work closely with the international community to put in place the international standards and frameworks needed to support these capacities over the long-term.

This work dates back to a DOE-developed task force in 1994 to mitigate the nuclear security vulnerabilities in the Former Soviet Union, which subsequently became the Material Protection, Control & Accounting (MPC&A) Program. In response to the attacks on September 11, 2001, the suite of technical assistance provided by MPC&A was modified to address the changing threat landscape. The primary change was to the approach, which developed into a graded, defense-in-depth security approach that begins at the source of the material outward, encompassing physical protection, material control & accounting, transportation security and response forces upgrades. The guiding principle of these efforts is to support improved security of nuclear and radiological material at the source, prior to it leaving the nuclear facility or site, which has been referred to as the first line of defense. However, recognizing this is not enough in light of continued smuggling activity and existence of materials out of regulatory control, DOE began the Second Line of Defense Program, which is now known as the Nuclear Smuggling Detection and Deterrence Program (NSDD).

NSDD is a critical component of overall U.S. efforts to counter nuclear smuggling. As a part of the Global Nuclear Detection Architecture (GNDA), NSDD works to judiciously deploy radiation detection systems internationally at official crossing points, along rugged, unofficial borders and disputed territories (i.e. “green” borders) and maritime borders (i.e. “blue” borders), and at internal locations for law enforcement operations. The GNDA is predicated on a layered defense of law enforcement, intelligence, and technology to maximize a system of detection and deterrence capability. DHS oversees the domestic layer of this architecture and the Departments of State, Energy, and Defense lead on the exterior layer in coordination with DHS. In the words of DNDO, NSDD “is the largest single program in the exterior layer and provides significant potential to stop a U.S.-bound terrorist attack outside our borders.”

NSDD has a long history of close collaboration with DHS, including both the Domestic Nuclear Detection Office (DNDO) and Customs and Border Protection (CBP). NSDD and DNDO regularly share information on their perception and definition of the threat and their prioritization methodologies for addressing the threat. NSDD and DNDO also collaborate on a number of technical and maintenance topics to leverage our respective experiences in deploying and maintaining large fleets of detection systems. Most recently, NSDD and DNDO signed an interagency Integrated Project Team Charter to jointly study the long-term effects of temperature fluctuations on the performance of radiation portal monitors. This allows us to share resources and work together to better understand an issue that will shape our approach to both procurement and long-term maintenance of these systems. With regard to collaboration with CBP, NSDD and CBP's Container Security Initiative (CSI) are working together collaboratively in many of the same seaports overseas. To coordinate our efforts, NSDD and CBP/CSI have a signed Standard Operating Procedures document that lays out how we share information, resources, and equipment to maximize our efforts to secure maritime cargo. As a final example, NSDD and the United Kingdom recently co-hosted an international workshop on enhancing maritime security that focused on promoting radiation detection in the maritime supply chain and developing enhanced measures to permanently remove materials found out of regulatory control. As a 2016 Nuclear Security Summit deliverable, 14 countries endorsed the best practices and recommendations from this workshop. DHS, both DNDO and CBP, played a critical role in this event and offered their insights, lessons learned and best practices to a group of over 15 countries and 9 international organizations dedicated to strengthening maritime security.

With regard to maritime security, it is important to note that the scanning of inbound containers at U.S. ports and border crossings is extremely important and crucial to our national defense, but the effectiveness of the systematic approach to detection is significantly strengthened by international efforts that extend detection away from U.S. soil. If an actual IND or RDD weapon reaches the U.S. shores, the detection may be too late to avoid its catastrophic consequences. In addition, the length of U.S. borders, along with the potential use of non-traditional delivery mechanisms such as light aircraft or small diesel powered submarines, makes securing the U.S. borders a difficult undertaking. Consequently, it is important for U.S. Government Agencies to collaborate effectively in the deployment of a layered defense that keeps materials secure *in situ*, but that also can prevent illicit trafficking internationally, at multiple vectors, at the farthest possible point from the U.S. border.

NSDD's role, working closely with DHS/DNDO and DOS, is to push the ring of security out as far as possible. The program has greatly contributed to building international awareness of nuclear threats and the capacity of the U.S. Government and partner countries to detect, deter, and investigate the illicit trafficking of nuclear and radioactive materials at international border crossings and internal partner country chokepoints. This has resulted in equipping 579 sites, including 45 large container seaports, and the provision of 102 mobile radiation detection vans.

But countering nuclear smuggling is not achieved by equipment alone. An effective Counter Nuclear Smuggling strategy involves coordination among many agencies and experts within partner countries; including border security, police, customs and security services, technical reach back, ministries of foreign affairs, and others. The United States Government interagency works in coordination to pursue this inclusive engagement, enabling a systematic approach where all kinds of capabilities are coordinated. NSDD plays a specific role in building capacity to counter nuclear smuggling and to link countries to international organizations, such as INTERPOL and the International Atomic Energy Agency (IAEA), in order to develop an integrated and cohesive community focused on combatting nuclear smuggling. To date, through its work with foreign partners NSDD has created a network of more than 100 agencies in 65 countries. NSDD has also transitioned sustainability responsibilities to approximately 85% of sites equipped.

NSDD supports this network by providing training, technical and best practices exchanges, workshops and exercises, assessment tools for tracking performance, and assistance with regulatory development. This ongoing engagement ensures a sustainable transition of responsibility for detection equipment to partners. It also allows NSDD to promote best practices in the long term and keep communication channels open to monitor trafficking incidents and evolving threat patterns.

I would like to draw your attention to a recent Government Accountability Office (GAO-16-460) report on the NSDD program, referencing three partner countries visited as part of the audit—Azerbaijan, Bulgaria, and Georgia. GAO reported that “law enforcement officers and government officials attributed multiple cases of successful detection, deterrence and seizure of smuggled nuclear and radiological materials to the use of NSDD-provided radiation detection equipment.” These nations all have both fixed site and mobile NSDD-provided detectors.

The development of robust and holistic counter nuclear smuggling capabilities also requires nuclear material analysis and characterization, also known as nuclear forensics. Attribution of interdicted material is key to identifying gaps in nuclear material security as well as enabling and supporting countries in their efforts to prosecute traffickers. In coordination with the Department of State, NSDD supports peer-to-peer efforts to broaden understanding of nuclear forensic signatures, provides technical expertise to support analytical capabilities and development of national nuclear forensics libraries, and supports development of international recommendations and implementing guidance through the IAEA and Global Initiative to Combat Nuclear Terrorism (GICNT).

DOE/NSA's technical capabilities and expertise at the national laboratories are essential to advancing NSDD's success in maximizing the performance of radiation detection equipment and advancing forensics. The laboratories test all equipment against rigorous performance standards, and maintain a feedback loop with vendors and maintenance providers in order to continuously improve detection capabilities and advance the user experience to make equipment easier to operate and maintain.

#### IV. STRATEGIC REVIEW AND PLANS

DNN's programs periodically undergo strategic reviews to assess progress, determine strategic direction, and recalibrate goals of the respective program's mission in light of the dynamic international threat environment. Related to the evolving nuclear smuggling threat landscape, NSDD conducted a strategic review in 2015 to assess progress and prioritize future work based on the current threat landscape.

The NSDD strategic review included qualitative (i.e., subject matter expertise) and quantitative (i.e., modeling) analyses. NSDD's conclusions were:

1. Radiological/nuclear smuggling threat is evolving, ungoverned spaces are expanding, and massive movements of people are overwhelming governments, particularly as this impacts border security;
2. It is imperative to test, qualify, and apply sustainable, flexible, and modular detection and identification technologies to address longstanding challenges;
3. The changed threat environment requires reinforcement of detection capabilities (strategic layering of fixed, mobile, and modular capability);
4. Maintaining insight into partner operation of systems is vitally important; and
5. The detection and deterrence value of radiation portal monitors (RPMs) continues to play a key role in the exterior and domestic layers of the GNDA.

NSDD plans include deploying radiation detection systems in critical pathways through the Fergana Valley in Central Asia, Ukraine, and Eastern Europe, along with targeted deployments at seaports in key regions. This includes continuing to deploy mobile detection systems to law enforcement to reinforce and complement the fixed radiation detection architecture established. This fixed and mobile work has been the traditional NSDD implementation approach, and with a focused effort during the next several years, much of this work will be completed. NSDD will continue to maintain strategic relationships that have been built which provide important insights into the counter smuggling challenges faced in various countries and regions. The program will continue to carry out technical and best practices exchanges with high income countries, such as China. These peer-to-peer engagements allow NSDD to share technical expertise, but we look to our partners to make the investments and have immediate responsibility for the maintenance and sustainment of any equipment.

NSDD's updated strategy includes a focus on partner countries that are "one-step out" from nuclear and radioactive source countries where bilateral cooperation efforts have not been successful. This ring approach has included an emphasis on using flexible and modular radiation detection tools in the maritime and air traffic vectors. The Strategic Airports Initiative is focused on expanding the application of radiation detection systems in the Middle East and South Asia, whereas the Maritime Vectors Partnership focuses on unregulated, open waterways that have the potential of linking source materials to potential users/buyers. The operational



approach to these maritime activities will be to expand use of radiation detection equipment for land based and at sea operations.

A key element of NSDD's activities with partner countries is their sustainability program. While we have reached an 85% transition point, continuing to make progress in transitioning this responsibility is a continued emphasis. NSDD's unique relationships with partners underscore the need to remain engaged after transition with bilateral, regional, and international partners to support continued effective use of deployed systems. NSDD will continue its work with partners to further develop their training programs, including conducting workshops, field and training exercises, and drills to continue to enhance the international capacity to detect and interdict nuclear smuggling.

NSDD, like our other DNN offices, will need to continue to expand its engagement with international organizations as force multipliers. This means collaborating on capacity building efforts with the IAEA, European Commission Joint Research Center (EC-JRC), GICNT, Global Partnership, and INTERPOL. As we look forward from the 2016 Nuclear Security Summit, these organizations will be champions of continuing the strides made in advancing the global nuclear security architecture under the Summit process and will be a key component of long-term nuclear security.

As a result of NSDD's strategic review, we believe that NSDD and programs like it must remain vigilant and responsive to the evolving threat landscape. We have found that our approach to tailoring technical capabilities to their location and function is successful. Based on feedback from our partners, RPMs continue to be a key tool in the technology component to counter nuclear smuggling of the GNDA because they drive smugglers toward riskier and costlier behavior that exposes them to law enforcement or other means of detection. When RPMs are combined with other mobile and portable detection tools, we are able to close off many of the pathways smugglers might use.

## **V. ADDITIONAL PROGRAMS**

Within DNN, there are complementary efforts that further the overall mission to detect, deter, and investigate illicit trafficking of nuclear and other radioactive material. Of particular note is the Commodity Identification Training (CIT) conducted by the Office of Nonproliferation and Arms Control. This course enhances the ability of enforcement personnel, primarily customs officers, to recognize and interdict strategic commodities. CIT Instructor Training prepares national specialists to provide CIT on a widespread basis and to provide support when inspectors request analysis of suspect items. This course is provided to many of the same partners as NSDD collaborates with and is another capacity that they develop in executing their overall border enforcement missions.

Also of note are the complementary international activities that are conducted by DOE/NNSA's Office of Counterterrorism and Counterproliferation (CTCP). This office is charged with

understanding nuclear threat devices (i.e., improvised nuclear devices, foreign nuclear weapons of a proliferant concern, and any device that may have fallen outside of a foreign state's custody). As this relates to NSDD, one area that CTCP is focused on is Emergency Response and Forensics. In accomplishing these missions, CTCP has collaborated with NSDD and its partners to provide technical expertise and collaboration on training, workshops, and other activities that further develop international nuclear nonproliferation capacity.

Beyond work within DOE/NNSA, we work with the Interagency to further enhance the capabilities of our partners. NSDD collaborates with the Department of State, Department of Defense, and FBI on field training exercises and workshops that focus on response plans and standard operating procedures, as they relate to radiation detection and border security. Depending on the event, each U.S. Government organization plays a different role and supports each other in these efforts. NSDD also regularly participates in coordination meetings with interagency counterparts.

An example of a NSDD collaboration with FBI is providing Radiation Detection and Investigative Techniques (RDIT) training to international partners. This training jointly provided by NSDD and FBI incorporates law enforcement elements into radiation detection operations and is extremely popular with our international partners.

Internationally, NSDD is involved with all of the major players who provide guidance and technical support on topics related to radiation detection and countering nuclear smuggling. This includes the IAEA, INTERPOL, EC-JRC, World Customs Organization (WCO), and GICNT. We provide subject matter experts to support training events, workshops, and guidance development.

#### **VI. RECENT HOUSE COMMITTEE ON ENERGY AND COMMERCE (HE&C) INTEREST AND THE GAO REPORT**

As you may know, bipartisan leaders of the HE&C sent a letter on May 2, 2016 to Secretary of Energy seeking further information on the current status of the DOE/NNSA NSDD programs. They noted that the purpose of the letter was in consideration of the fact that "recent international developments—particularly the rise of well-funded terror groups and the curtailment of U.S.-Russian cooperation on nuclear material security—have underscored the importance of NNSA's Nuclear Smuggling Detection and Deterrence (NSDD) programs." They noted that information reviewed to date has highlighted the importance of maintaining a strong deterrence and detection posture at foreign ports and border crossings, in partnerships with other nations, and mentioned that "given the current threat environment, now is not the time to weaken our detection and interdiction programs overseas." NSDD provided some follow-up briefings and will be providing additional information in response to the HE&C Committee's request.

As I mentioned earlier in this testimony, GAO recently completed an audit on NSDD. We were pleased that the audit underscored the importance of NSDD's work to enhance the global nuclear security architecture. The conclusion in particular noted that "NSDD plays a key role in building the capacity of its 59 partner countries to detect, interdict, and investigate the illicit trafficking of nuclear and radiological materials, and the use of NSDD-provided equipment has resulted in positive outcomes, including the interdiction of weapons-grade HEU."

## **VII. CONCLUSION**

The threat posed by nuclear terrorism remains. Terrorist groups have sought nuclear and radiological materials and the expertise needed to weaponize them. Without the long-standing cooperation to improve the security of Russian weapons-useable materials, security conditions may weaken. Terrorist groups are taking root in under-governed spaces that hold radiological materials of concern. All of these facts underscore a critical component of U.S. national security strategy is to prevent the illicit trafficking of nuclear and radiological materials. This challenge is dynamic and requires a broad set of capabilities to be effective.

We have taken important steps forward in countering this threat through the deployment of detection systems, development of competent partners, and advancement of nuclear forensics capabilities. Through its strategic review, NSDD has further identified ways to lead the global effort to combat nuclear smuggling while remaining agile and responsive to the shifting threat landscape. The GAO report, while overwhelmingly positive, identified areas where NSDD can apply more rigorous tracking of milestones and goals, and NSDD is taking steps to respond to this guidance. Given NSDD's ability to adapt, widespread and diverse international partnerships, and ongoing collaboration with interagency partners, NSDD is uniquely poised to remain the global leader in deploying and sustaining the global nuclear detection architecture with the ultimate goal of preventing the use of a nuclear weapon or dirty bomb in the United States.

Thank you for the opportunity to appear before you today. I am happy to answer any questions.



---

United States Government Accountability Office

Testimony

Before the Subcommittees on Coast Guard and Maritime Transportation and Border and Maritime Security, Committees on Transportation and Infrastructure and Homeland Security, House of Representatives

---

For Release on Delivery  
Expected at 10:00 a.m. ET  
Thursday, July 7, 2016

## MARITIME SECURITY

# Progress and Challenges in Implementing Maritime Cargo Security Programs

Statement of Jennifer A. Grover, Director  
Homeland Security and Justice

## GAO Highlights

Highlights of GAO-16-790T, a testimony before the Subcommittees on Coast Guard and Maritime Transportation and Border and Maritime Security, Committees on Transportation and Infrastructure and Homeland Security, House of Representatives

### Why GAO Did This Study

The U.S. economy is dependent on the expeditious flow of millions of tons of cargo each day through the global supply chain—the flow of goods from manufacturers to retailers. Criminal or terrorist attacks using cargo shipments can cause disruptions to the supply chain and can limit global economic growth and productivity. Within DHS, CBP has responsibility for administering maritime cargo security measures and reducing the vulnerabilities associated with the supply chain. CBP has developed a layered security strategy that focuses its limited resources on targeting and examining high-risk cargo shipments that could pose a risk while allowing other cargo shipments to proceed without unduly disrupting commerce arriving in the United States.

This statement discusses the progress and challenges associated with CBP's implementation of initiatives and programs responsible for enhancing the security of the global supply chain. The statement is based on reports and testimonies GAO issued from April 2008 through January 2015 related to maritime cargo security—with selected updates on how DHS has responded to GAO's prior recommendations.

### What GAO Recommends

In prior reports, GAO has made recommendations to DHS to strengthen various maritime cargo security programs. DHS generally concurred with the recommendations and has taken actions, or has actions under way, to address many of these recommendations.

View GAO-16-790T. For more information, contact Jennifer A. Grover at (202) 512-7141 or grovenj@gao.gov.

July 7, 2016

## MARITIME SECURITY

### Progress and Challenges in Implementing Maritime Cargo Security Programs

#### What GAO Found

The Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) have made substantial progress in implementing initiatives and programs that, collectively, have enhanced cargo security, but some challenges remain. Examples of progress and challenges are discussed below.

**Risk Assessments of Cargo Shipments.** In January 2015, GAO found that CBP did not have accurate data on the number and disposition of each high-risk shipment scheduled to arrive in the United States. Specifically, CBP's data overstated the number of high-risk shipments, including those that appeared not to be examined or waived in accordance with CBP policy. CBP officers inconsistently applied criteria to make some waiver decisions and incorrectly documented waiver reasons. GAO recommended that CBP define waiver categories and disseminate policy on issuing waivers. In response, CBP issued a new policy that includes criteria for waiving examinations of high-risk shipments and developed a new process for recording waivers and issued a memorandum.

**Partnerships with Foreign Governments.** In September 2013, GAO reported that CBP had not regularly assessed foreign ports for risks to cargo since 2005. GAO recommended that DHS periodically assess the security risks from ports that ship cargo to the United States and use the results to inform whether changes need to be made to Container Security Initiative (CSI) ports. DHS concurred with the recommendation and CBP has since developed a port risk matrix and priority map to be used to help assess whether changes need to be made to CSI ports. These tools are to be updated yearly and can be updated more frequently based on significant changes, emerging threats, and intelligence. These tools should assist CBP in ensuring it is allocating its resources to provide the greatest coverage of U.S.-bound high-risk cargo.

In October 2009, GAO reported challenges to scanning 100 percent of U.S.-bound cargo at foreign ports. DHS officials acknowledged that most, if not all foreign ports, would not be able to meet the July 2012 target date for scanning all U.S.-bound cargo, and DHS would need to issue extensions to allow the continued flow of commerce and remain in compliance with statutory requirements. Although the Secretary of Homeland Security has issued three 2-year extensions for implementing the 100 percent scanning mandate, which have extended the deadline to July 2018, DHS has not yet identified a viable solution to meet the requirement.

**Partnerships with the Trade Industry.** Through the Customs-Trade Partnership Against Terrorism (C-TPAT) program, CBP officials work with member companies to validate the security of their supply chains in exchange for benefits, such as reduced scrutiny of their shipments. In April 2008, GAO found, among other things, that CBP lacked a systematic process to ensure that members take appropriate actions in response to security validations. GAO recommended that CBP document key data elements needed to track compliance. CBP has since implemented a process to ensure that C-TPAT validation report recommendations are implemented. GAO is currently reviewing the C-TPAT program, to include an assessment of CBP's ability to meet its security validation responsibilities.

United States Government Accountability Office

---

Chairman Hunter, Chairwoman McSally, Ranking Members Garamendi and Vela, and Members of the Subcommittees:

Thank you for the opportunity to discuss our work on U.S. Customs and Border Protection's (CBP) initiatives and programs to enhance maritime cargo security. The U.S. economy is dependent on the expeditious flow of millions of tons of cargo each day through the global supply chain—the flow of goods from manufacturers to retailers. Cargo containers are an important segment of the global supply chain and play a vital role in the movement of cargo between global trading partners. The majority of U.S. imports arrive by ocean vessel, and much of that is shipped in the millions of cargo containers that enter the United States every year. Cargo containers can be filled overseas at many different locations and they are transported through complex logistics networks before reaching U.S. ports. Criminal or terrorist attacks using cargo shipments can cause disruptions to the supply chain and can limit global economic growth and productivity.<sup>1</sup> Within the Department of Homeland Security (DHS), CBP is responsible for administering cargo security and reducing the vulnerabilities associated with the supply chain. According to DHS, balancing security concerns with the need to facilitate the free flow of commerce, part of CBP's mission, remains an ongoing challenge.<sup>2</sup>

CBP has developed a layered security strategy to focus its limited resources on targeting and examining high-risk cargo shipments that could pose a risk while allowing other cargo shipments to proceed without unduly disrupting commerce arriving in the United States. CBP's layered security strategy is based on initiatives and programs that include, among other things, analyzing information to identify shipments that may be at high risk of transporting weapons of mass destruction (WMD) or other contraband, working with foreign governments to examine U.S.-bound shipments at foreign ports participating in the Container Security Initiative (CSI) and Secure Freight Initiative (SFI), and providing benefits to companies that comply with CBP's minimum security criteria through the

---

<sup>1</sup>The White House, *National Strategy for Global Supply Chain Security* (Washington, D.C.: January 2012).

<sup>2</sup>In addition to its priority mission of keeping terrorists and their weapons out of the United States, CBP is also responsible for securing the border, facilitating international trade and travel, collecting duties, and enforcing numerous U.S. laws and regulations pertaining to immigration and illicit drugs, among other things.

---

Customs-Trade Partnership Against Terrorism (C-TPAT) program. The Security and Accountability for Every Port Act (SAFE Port Act) of 2006, enacted in October 2006, established a statutory framework for key programs within CBP's layered security strategy that previously had not specifically been required by law.<sup>3</sup> A brief description of the key initiatives and programs that constitute CBP's layered security strategy is provided in appendix I.

My statement today discusses the progress and challenges associated with CBP's implementation of maritime cargo security initiatives and programs responsible for enhancing the security of the global supply chain. This statement is based on reports and testimonies we issued from April 2008 through January 2015 related to maritime cargo security—with selected updates on how DHS and CBP have responded to our prior recommendations. The products cited in this statement provide detailed information on our scope and methodology. The work upon which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

Every time responsibility for cargo changes hands along the global supply chain there is the potential for a security breach. As a result, vulnerabilities exist that terrorists could take advantage of by, for example, placing a WMD into a container bound for the United States. While there have been no known incidents of containers being used to transport WMD, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. To address the potential security risks posed by the millions of containers that arrive in the United States each year, CBP has implemented a layered security strategy of related initiatives and programs that focus CBP's limited resources on potentially high-risk cargo bound for the United States while allowing other cargo to proceed without undue

---

<sup>3</sup>Pub. L. No. 109-347, 120 Stat. 1884 (2006).

---

disrupting commerce. Key elements of CBP's maritime cargo security initiatives and programs are described below.

**Automated Targeting System.** Information on shipments destined for the United States is automatically fed into CBP's Automated Targeting System (ATS)—an enforcement and decision support system that compares cargo information against intelligence and other law enforcement data. ATS consolidates data from various sources to create a single, comprehensive record for each U.S.-bound shipment. ATS uses a set of rules that assess different factors in the information to determine the risk level of a shipment. One set of rules within ATS, referred to collectively as the maritime national security weight set, is programmed to check for information or patterns that could be indicative of suspicious or terrorist activity. ATS uses this weight set to assess and generate risk scores for every cargo shipment as the shipment moves throughout the global supply chain and new information is provided or existing information is revised. CBP classifies the risk scores from the maritime national security weight set as low, medium, or high risk. ATS automatically places high-risk shipments on hold, and CBP officials use information in ATS to identify (target) which high-risk shipments should be examined or waived.

To assist in its targeting efforts, CBP uses key information about shipments destined for the United States obtained through the 24-hour rule and the 10+2 rule. Through the 24-hour rule, CBP generally requires vessel carriers to electronically transmit cargo manifests to CBP 24 hours before cargo is loaded onto U.S.-bound vessels at foreign ports.<sup>4</sup> Through the Importer Security Filing and Additional Carrier Requirements (known as the 10+2 rule), CBP requires importers and vessel carriers to provide data elements for improved identification of cargo shipments that may pose a risk for terrorism.<sup>5</sup> Importers are responsible for supplying CBP with 10 shipping data elements—such as country of origin—24 hours prior to loading, while vessel carriers are required to provide 2 data

---

<sup>4</sup>19 C.F.R. § 4.7(b). Cargo manifests are prepared by the ocean carrier and are composed of bills of lading for each shipment loaded onto a vessel to describe the contents of the shipments. Bills of lading are documents issued by a carrier describing the goods, the details of the intended voyage, and the conditions of transportation.

<sup>5</sup>Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (codified at 19 C.F.R. pt. 149).



---

elements—container status messages and stow plans—that are not required by the 24-hour rule.<sup>6</sup>

**Container Security Initiative.** CSI is a bilateral government partnership program operated by CBP that aims to identify and examine U.S.-bound cargo container shipments that are at risk of containing WMD or other terrorist contraband. As part of the program, CBP officers are stationed at select foreign seaports and review information about U.S.-bound containerized cargo shipments. CBP uses ATS to target U.S.-bound container shipments and request examinations of high-risk container shipments before they are loaded onto vessels. CSI is operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CBP estimates that, through the CSI program, it prescreens over 80 percent of all maritime containerized cargo imported into the United States.

**Secure Freight Initiative.** In response to a requirement in the SAFE Port Act to scan 100 percent of U.S.-bound cargo containers, CBP established SFI.<sup>7</sup> CBP uses radiation detection and non-intrusive inspection equipment to scan cargo containers before they are loaded onto vessels at select foreign seaports. Radiation detection equipment, such as radiation portal monitors (RPM) and radiation isotope identification devices (RIID) detect the presence of radioactive material that may be in a container. RIIDs and certain types of RPMs can identify the specific radioactive isotope being emitted and whether the radiation is a threat or is naturally occurring, such as that found in certain ceramic tiles. The second type of equipment, referred to as non-intrusive inspection equipment, uses X-rays or gamma rays to scan a container and produce images of a container's contents without having to open it.

**Customs-Trade Partnership Against Terrorism.** C-TPAT is a voluntary, public-private sector partnership with private stakeholders in the

---

<sup>6</sup>Container status messages report terminal container movements, such as loading and discharging the vessel, and report the change in the status of containers, such as if they are empty or full. Container status messages also report conveyance movements, such as vessel arrivals and departures. A vessel stow plan includes information such as the vessel operator, voyage number, the stow position of each container, hazardous material code (if applicable), and the port of discharge.

<sup>7</sup>See 6 U.S.C. §§ 981-82.

---

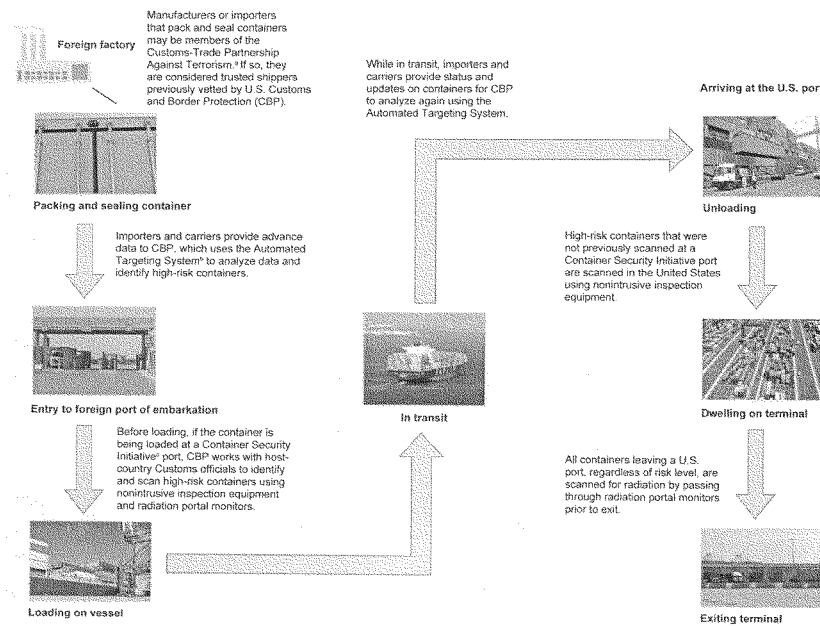
international trade community that aims to secure the flow of maritime cargo bound for the United States.<sup>8</sup> Through C-TPAT, CBP officials work with member private companies to review the security of their supply chains to ensure their security practices meet CBP's minimum security criteria. In return, C-TPAT members receive various benefits, such as reduced scrutiny of their shipments.

Figure 1 provides an overview of the global supply chain and the steps in the supply chain where CBP's key initiatives and programs come into play.

---

<sup>8</sup>See 6 U.S.C. § 961.

Figure 1: The Global Supply Chain and CBP's Key Cargo Security Initiatives and Programs



Source: GAO (analysis); GAO and Department of Homeland Security Science and Technology Directorate (photos); Art Explosion (clipart). | GAO-16-790T

<sup>1</sup>The Customs-Trade Partnership Against Terrorism is a voluntary program designed to improve the security of the supply chain while maintaining an efficient flow of goods. Under this program, CBP officials work in partnership with private companies to review their supply chain security plans to improve members' overall security.

<sup>2</sup>The Automated Targeting System is a mathematical model that uses weighted rules to assign a risk score to arriving cargo shipments based on shipping information. CBP uses the Automated Targeting System as a decision support tool in targeting cargo containers for inspection.

<sup>3</sup>The Container Security Initiative places CBP staff at participating foreign ports to work with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before it is shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that the officials' foreign counterparts examine the contents of the containers.

---

### CBP Has Made Substantial Progress in Enhancing Cargo Security, but Some Challenges Remain

Our prior work has shown that CBP has made substantial progress in implementing various initiatives and programs that, collectively, have enhanced cargo security, but some challenges remain. Examples of progress and challenges in the areas of (1) using information for improving targeting and risk assessment of cargo shipments, (2) partnerships with foreign governments, and (3) partnerships with the trade industry are discussed below.

---

### CBP's Efforts to Improve Targeting and Risk Assessments of Cargo Shipments

In January 2015, we found, among other things, that CBP did not have accurate data on the number and disposition of each high-risk maritime cargo shipment scheduled to arrive in the United States.<sup>9</sup> On the basis of our analyses of CBP data for fiscal years 2009 through 2013, we found that, on average each year, approximately 11.6 million maritime cargo container shipments arrived in the United States, and less than 1 percent of those shipments were determined by ATS to be high-risk. We found that CBP examined the vast majority of high-risk shipments, but CBP's data on the disposition of high-risk shipments were not accurate because of various factors, such as the inclusion of shipments that were never sent to the United States. Further, our analyses found that CBP's data overstated the number of high-risk shipments, including those that appeared not to be resolved (examined or waived) in accordance with CBP policy. We also found that when determining the disposition of high-risk shipments, CBP officers were inconsistently applying criteria to make some waiver decisions and were also incorrectly documenting the reasons for waivers.<sup>10</sup> As a result, we concluded that CBP could not accurately determine the extent to which waivers were used consistently and judiciously across CBP targeting units, as required by policy. We recommended, among other things, that CBP define waiver categories

---

<sup>9</sup>GAO, *Supply Chain Security: CBP Needs to Enhance Its Guidance and Oversight of High-Risk Maritime Cargo Shipments*, GAO-15-294 (Washington, D.C.: Jan. 27, 2015).

<sup>10</sup>CBP officers can waive an examination if they determine through research that (1) the shipment falls within a predetermined category of stated exceptions (standard exception), or (2) they can articulate why the shipment should not be considered high-risk (articulable reason). For example, a shipment could be identified as high-risk because it is associated with a shipper on a terrorist watch list, but through further research, CBP officials determine the shipper is not a true match to the terrorist watch list and, therefore, the shipment should not be considered high-risk.

---

and disseminate policy on issuing waivers for high-risk shipments. DHS concurred with our recommendations and, in December 2015, CBP issued a new policy, *National Security Cargo Targeting Procedures*, that includes criteria for waiving mandatory examinations of high-risk shipments (referred to as exceptions). The new policy also specifically identifies certain types of shipments that do not qualify for exceptions to examination requirements. In addition, CBP developed a new process for recording waivers and issued a memorandum to targeting units on how to apply the new procedures. CBP's actions help ensure that all of its targeting units are correctly and consistently applying and documenting waivers.

In October 2012, we found that more regular assessments of ATS were needed to enhance CBP's targeting of maritime cargo and better position CBP to provide reasonable assurance of the effectiveness of ATS.<sup>11</sup> We, therefore, recommended that CBP (1) ensure that future updates to the rules that identify risks are based on results of assessments that demonstrate the effectiveness of such updates; and (2) establish targets for CBP's performance measures and use those measures to assess the effectiveness of ATS on a regular basis to better determine when updates to the rules that identify risks are needed. DHS concurred with the recommendations and, in May 2015, CBP revised its *National Security Weight Set, Maritime Standard Operating Procedures* (SOP) to address the new requirements for the maintenance, review, and update of the national security weight set in ATS. The SOP requires program managers to compare proposed versions of the national security weight set against the existing version as part of the process for determining whether to implement a proposed new version of the weight set. Doing so will help provide reasonable assurance that changes to the weight set will improve the effectiveness of CBP's targeting of maritime cargo container shipments. The SOP also establishes a performance measure and an associated target that will assist CBP in determining whether the weight set is effectively targeting maritime cargo container shipments. The SOP requires CBP to review the national security weight set for revisions if the weight set does not meet the performance target in two consecutive quarters. By assessing the weight set regularly against a performance

---

<sup>11</sup>GAO, *Supply Chain Security: CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System*, GAO-13-9 (Washington, D.C.: Oct. 25, 2012).

---

target, CBP will be better positioned to determine when updates to the weight set are needed to ensure continued effectiveness in targeting of high-risk maritime cargo container shipments.

In September 2010, we reviewed CBP's efforts to collect additional data through the 10+2 rule and utilize these data to identify high-risk shipments.<sup>12</sup> We found that the 10+2 rule data elements were available for identifying high-risk cargo, but CBP had not yet finalized its national security targeting criteria to include these additional data elements to support high-risk targeting. We recommended that CBP establish milestones and time frames for updating the targeting criteria. In December 2010, CBP provided us with a project plan for integrating the data into its criteria, and in January 2011, CBP implemented the updates to address risk factors present in the 10+2 data. We are currently reviewing CBP's implementation and enforcement of the 10+2 program and anticipate issuing our report in spring 2017.

---

#### CBP's Partnerships with Foreign Governments

In September 2013, we reported on CBP's progress in implementing CSI.<sup>13</sup> Specifically, we found that CBP had not regularly assessed foreign ports for risks to cargo under the CSI program since 2005. While CBP took steps to rank ports for risks in 2009, we found that CBP did not use results from this assessment to make modifications to the locations where CSI staff are posted because of budget cuts. By applying CBP's risk model to fiscal year 2012 cargo shipment data, we found that CSI did not have a presence at about half of the foreign ports CBP considered high-risk, and about one-fifth of the existing CSI ports were at lower-risk locations. We recommended that DHS periodically assess the supply chain security risks from all foreign ports that ship cargo to the United States and use the results of these risk assessments to inform any future expansion of CSI to additional locations and determine whether changes need to be made to existing CSI ports and make adjustments as appropriate and feasible. DHS concurred with our recommendation and,

---

<sup>12</sup>GAO, *Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain*, GAO-10-841 (Washington, D.C.: Sept. 10, 2010).

<sup>13</sup>GAO, *Supply Chain Security: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports*, GAO-13-764 (Washington, D.C.: Sept. 16, 2013).

---

in response, CBP developed a CSI Port Risk Matrix and Port Priority Map. CBP officials stated that the matrix and map will be used, along with several other tools available to CSI, to assess whether changes need to be made to CSI ports worldwide. According to CBP, these tools are to be updated yearly and, if necessary, can be updated more frequently based on significant changes, emerging threats, and intelligence. As a result of developing and employing these new risk-assessment tools, CBP should be better positioned to ensure that it is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing WMD or other terrorist contraband into the United States through the supply chain.

In October 2009, we reported that scanning operations at the initial SFI ports encountered a number of challenges—including safety concerns, logistical problems with containers transferred from rail or other vessels, scanning equipment breakdowns, and poor-quality scan images.<sup>14</sup> Both CBP and GAO had previously identified many of these challenges, and CBP officials were concerned that they and the participating ports could not overcome them. Senior DHS and CBP officials acknowledged that most, if not all foreign ports, would not be able to meet the July 2012 target date for scanning all U.S.-bound cargo, and DHS would need to issue extensions to such ports to allow the continued flow of commerce in order to remain in compliance with relevant statutory requirements.<sup>15</sup> We recommended that DHS, in consultation with the Secretaries of Energy and State, develop, among other things, more comprehensive cost estimates, conduct cost-benefit and feasibility analyses, and provide the results to Congress. In response to our recommendations, CBP stated it had no plans to develop comprehensive cost estimates or feasibility analyses since SFI is operating at one port and it had no funds to conduct

---

<sup>14</sup>GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

<sup>15</sup>Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007, which established the July 2012 deadline for 100 percent scanning of containers loaded in a port or ports, this deadline may be extended in two-year increments if DHS certifies to Congress that at least two out of a list of specific conditions exist. Among others, these conditions include the following: adequate scanning equipment is not available or cannot be integrated with existing systems, a port does not have the physical characteristics to install the equipment, or use of the equipment will significantly affect trade capacity and the flow of cargo. See 6 U.S.C. § 982(b)(4).

---

such analyses. In July 2013, we closed these recommendations as not implemented.

In May of 2012, 2014, and 2016, the Secretary of Homeland Security authorized a 2-year extension of the deadline for implementing the 100 percent scanning requirement for U.S. bound cargo before it is loaded onto vessels at foreign seaports. In May 2014, the Secretary of Homeland Security renewed the extension (until July 2016) and stated that "DHS's ability to fully comply with this unfunded mandate of 100 percent scanning, even in [the] long term, is highly improbable, hugely expensive, and in our judgment, not the best use of taxpayer resources to meet this country's port security and homeland security needs." The Secretary also stated that he instructed DHS, including CBP, to do a better job of meeting the underlying objectives of the mandate. In the most recent letter, dated May 2016, authorizing the extension until July 2018, the Secretary stated he has committed the Department to work towards meeting the mandated 100 percent scanning requirement. The Secretary also outlined steps DHS is taking to engage stakeholders to identify solutions by leveraging the private sector. DHS plans to assess the feedback it receives during the summer of 2016 and will subsequently seek to test viable solutions in operational environments.

---

**CBP's Partnerships with  
the Trade Industry**

In April 2008, we reported, among other things, that CBP took steps to improve the process for validating C-TPAT applicants' security practices and implemented numerous actions to address C-TPAT management and staffing challenges.<sup>16</sup> However, we found challenges with the technology CBP used to help ensure that validation information is consistently collected, documented, and uniformly applied to decisions regarding the awarding of benefits to C-TPAT members, and that CBP lacked a systematic process to ensure that members take appropriate actions in response to security validation findings. We also found that C-TPAT's performance measures were insufficient to assess the impact of C-TPAT on increasing supply chain security. We made recommendations to CBP to strengthen C-TPAT program management and oversight. Specifically, we recommended, among other things, that CBP document

---

<sup>16</sup>GAO, *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, GAO-08-240 (Washington, D.C.: Apr. 25, 2008).



---

key data elements needed to track compliance with the SAFE Port Act and other CBP internal requirements and to identify and pursue opportunities in information collected during C-TPAT member processing activities that may provide direction for developing performance measures of enhanced supply chain security. CBP has since implemented these recommendations by, for example, creating an automated platform to track and capture the content and communication between CBP and C-TPAT members to ensure that C-TPAT validation report recommendations are implemented and identifying analytical tools and data for trend analysis to better assess C-TPAT's impact on the supply chain. We are currently reviewing the C-TPAT program, specifically how CBP assesses member benefits and conducts security validation responsibilities. We anticipate issuing our report in late fall 2016.

---

Thank you Chairman Hunter, Chairwoman McCally, Ranking Members Garamendi and Vela, and Members of the Subcommittees. This completes my prepared statement. I would be happy to respond to any questions you may have at this time.

---

#### GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Christopher Conrad (Assistant Director), Carla Brown, Lisa Canini, Michele Fejfar, Eric Hauswirth, Heidi Nielson, Ashley Rawson, and Natarajan Subramanian. Key contributors for the previous work that this testimony is based on are listed in those products.

## Appendix I: Description of CBP's Layered Security Strategy for Maritime Cargo Shipments

This appendix describes the key initiatives and programs related to U.S. Customs and Border Protection's (CBP) strategy for ensuring the security of maritime cargo. CBP has developed this strategy to mitigate the risk of weapons of mass destruction, terrorist-related material, or other contraband from being smuggled into the United States. CBP's strategy is based on related initiatives and programs that attempt to focus resources on high-risk shipments while allowing other cargo shipments to proceed without unduly disrupting the flow of commerce into the United States. The strategy includes obtaining cargo information on shipments in advance of their arrival at U.S. ports to identify high-risk shipments, using technology to inspect cargo, and partnering with foreign governments and members of the trade industry. Table 1 provides a brief description of some of the key initiatives and programs that compose this security strategy.

**Table 1: Description of U.S. Customs and Border Protection's (CBP) Key Cargo Security Initiatives and Programs**

Initiative/program and year introduced	Description
<b>Obtaining advanced information to identify high-risk cargo</b>	
Automated Targeting System (ATS), 1999	ATS is an enforcement and decision support system that compares traveler, cargo, and conveyance information against intelligence and other enforcement data by incorporating risk-based targeting scenarios and assessments. ATS assigns a risk score to arriving cargo shipments based on shipping information to help CBP identify and prevent potential terrorists and terrorist weapons from entering the United States.
24-hour rule, 2002	CBP generally requires vessel carriers to electronically transmit cargo manifests to CBP's Automated Manifest System 24 hours before U.S.-bound cargo is loaded onto a vessel at a foreign port. The information is used by ATS in its calculation of risk scores. The cargo manifest information is submitted by vessel carriers for all arriving cargo shipments.
Importer Security Filing and Additional Carrier Requirements (also known as the 10+2 rule), 2009	CBP requires importers and vessel carriers to provide data elements for improved identification of containerized shipments that may pose a risk for terrorism. The importer is responsible for supplying CBP with 10 shipping data elements, such as country of origin, 24 hours prior to loading, while the vessel carrier is required to provide 2 data elements, container status messages and stow plans, not required by the 24-hour rule. <sup>3</sup>
<b>Domestic scanning technology deployments</b>	
Non-intrusive inspection (NII) equipment, 2001	CBP uses NII equipment to actively scan both randomly selected containers and those identified by ATS as high risk. NII uses X-rays or gamma rays to scan a container and create images of the container's contents without opening it. According to CBP, as of August 2014, it had deployed 272 large-scale NII systems to U.S. seaports to scan containers.
Radiation portal monitors (RPM), 2002	CBP's program to scan 100 percent of containers arriving in the United States with radiation detection equipment prior to leaving a domestic port. As of August 2014, the Department of Homeland Security (DHS) had deployed 388 radiation portal monitors at U.S. seaports, through which over 99 percent of all containerized cargo arriving by sea is scanned.
<b>Partnerships with foreign governments and the trade industry</b>	

---

**Appendix I: Description of CBP's Layered  
Security Strategy for Maritime Cargo  
Shipments**

---

Container Security Initiative, 2002	CBP places staff at participating foreign ports to work with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that their foreign counterparts examine the contents of the containers. As of July 2014, there were 58 Container Security Initiative ports located in 32 countries.
Secure Freight Initiative (SFI), 2007	CBP initiative to scan 100 percent of U.S.-bound container cargo for nuclear and radiological materials at selected foreign ports using integrated examination systems that couple NII and radiation detection equipment before being placed on U.S.-bound vessels. <sup>6</sup> SFI was originally operational at six ports, but has since been reduced in scope and is only operational at one port.
Customs-Trade Partnership Against Terrorism, 2001	CBP develops voluntary partnerships with members of the international trade community composed of importers; manufacturers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies that implement specific security measures and best practices receive facilitated processing, such as a reduced likelihood of security-based examinations of their cargo.

Source: GAO summary of information provided by the Department of Homeland Security. | GAO-16-790T.

<sup>6</sup>Container status messages report terminal container movements, such as loading and discharging the vessel, and report the change in the status of a container, such as if it is empty or full. The stow plan provides information on the position of each cargo container on a vessel.

<sup>7</sup>See 6 U.S.C. § 982 (stating the July 2012 deadline for 100 percent scanning of containers loaded in a port or ports, and allowing this deadline to be extended in two-year increments if DHS certifies to Congress that at least two out of a list of specific conditions exist).



---

**GAO's Mission**

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

**Obtaining Copies of GAO Reports and Testimony**

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

---

**Order by Phone**

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

**Connect with GAO**

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts and read The Watchblog. Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

**To Report Fraud, Waste, and Abuse in Federal Programs**

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

**Congressional Relations**

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

**Public Affairs**

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548



Please Print on Recycled Paper.

## **Remote Detection of Concealed Nuclear Material**

Dr. Gregory H. Canavan

1. The need to detect concealed nuclear materials became clear on 9/11. My testimony to the Subcommittee on Coast Guard and Maritime Transportation on 27 October 2015 argued that fast neutrons could produce the high signal to noise ratios (SNR) needed for confident detection of nuclear devices in transportation containers. The analysis here indicates that is also possible for devices with significant countermeasures intended to reduce nuclear signatures and energies. Fast neutrons could fill TEU with neutrons that penetrate concealing moderators and cores, produce fission, and generate distinct signals at distant sensors. Fast neutrons produce fission neutrons whose energy difference forms the basis for robust detection of nuclear material. Fast neutron diffusion through moderators reduces their number but increases energy differences, which assists detection.

2. Fast neutrons can penetrate  $\approx 30$  centimeters of moderators deployed to reduce neutrons flux and energy and yet retain enough of each for detection. Thicker moderators produce high SNR signals whose energy bands indicate moderator composition and intensity indicates thicknesses.

3. Adding moderator to an initially sub-critical device shifts it towards criticality and increases external signatures. For a solid-core device with 10% safety margin an additional 15 cm moderator could shift it back to critical, which could be compounded by container materials. Concealment has a price.

4. Neutron multiplication in the core can be estimated with standard models, which indicate that it is well below unity. Thus, neutron interrogation could not induce criticality.

5. Detection depends on the ratio of the difference between source and fission neutron energies to their combined

standard deviation. Those of fission neutrons fall exponentially with the number of collisions they experience in diffusing out through the moderator, so their averages are only  $\approx 1\%$  of their peaks, which contributes to high SNR.

6. Source neutron energies over 1 MeV are far above the averages for fission neutrons. Added to the result that fission standard deviations are small, that leads to detection SNR above 100. While source energies are in the MeVs and their collisions occur in microseconds, the measurements for discrimination are on fission neutrons at keV on time scales of milliseconds, which are conventional.

7. An order of magnitude change in fission statistics does not degrade SNR significantly. A 10-fold increase in average fission energy and standard deviation would shift the energy for SNR = 100 from 1 to 3 MeV; a 30-fold increase would only shift it to 5 MeV. A 100-fold increase would shift it to  $\approx 10$  MeV, but SNR = 100 is apparently possible even there.

8. X-rays can detect but cannot identify mass. Passive sensors do not detect materials with low emissions. Thermal neutrons can penetrate but are easily countermeasured.

9. Fast neutrons can penetrate over 30 cm concealment with currents, energies, and high SNR for confident detection. Their sources could be adapted from conventional well logging devices and their detectors from reactor and high energy instrumentation. They could be deployed on cranes, ships, or in ports for fast inspection of all cargo containers for confident detection of nuclear threats attempting to take advantage of the large number of containers entering U.S. ports.

### Figure captions

1. Fast neutrons slowing down in materials resembling the contents of typical TEU ( $\approx 5\%$  density Fe, for which the mean free path is  $\approx 1.5$  m) produce a roughly uniform distribution of neutrons in TEU sized volumes. Their energy falls from 14 MeV to 6 MeV in  $\approx 1$  microsecond where fission neutrons are  $< 1$  MeV. As both slow down they maintain a separation in energy that provides a basis for filtering. Source neutrons must diffuse through moderators, fission, and diffuse out for detection, which happens in less than a microsecond. Fast reactor theory can treat the slowing down of both the source and fission neutrons that represent the signal and noise. (G. Canavan, Remote Detection of Nuclear Material, Subcommittee on Coast Guard and Maritime Transportation, 27 October 2015)

2. Nuclear theory can treat the penetration of neutrons into moderators of varying thicknesses as a function of energy. For 5 cm carbon moderator (essentially a bare device) there is little attenuation. For 15 cm about 10% penetrates with 1 MeV energy left; for 30 cm about 0.1% penetrates. Thicker moderators produce high SNR signals that give information on their composition and thickness (E. Fermi Nuclear Physics)

3. There are constraints on concealment. A device with 4.5 cm core and 11.5 cm moderator radius whose fission probability is reduced 5% for safety would be returned to criticality by an additional 5 cm of moderator. One reduced by 10% would be returned to critical by 15 cm. (R. Serber, Los Alamos Primer, LA-1)

4. Neutron multiplication can be estimated with 6-factor models that reduce here to  $f = \nu pq$ , where  $\nu$  is the number of neutrons per fission,  $p$  is the probability of fission ( $\approx 1$  for highly enriched material) and  $q$  is the non-escape probability (1 for infinite media and  $\approx 1/\nu$  near criticality.) For stability  $f < 1$ , or  $pq < 1/\nu$ , where  $\nu = 2.9$  for plutonium and 2.4 for

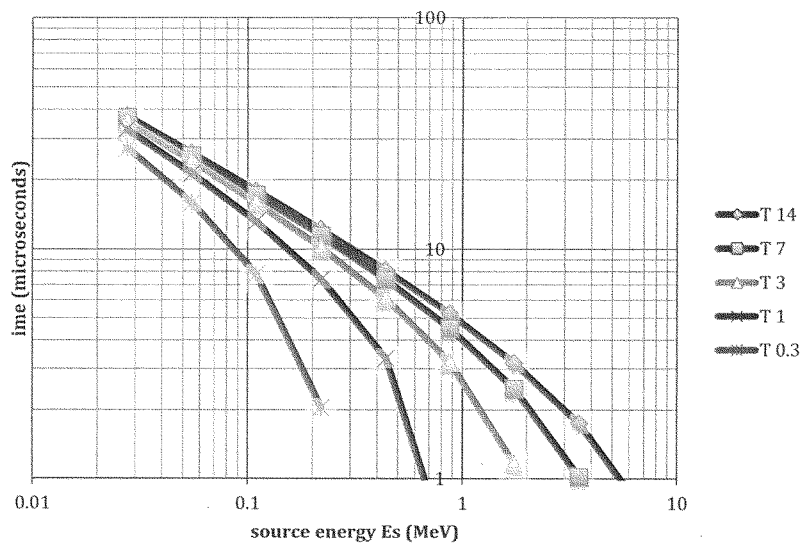
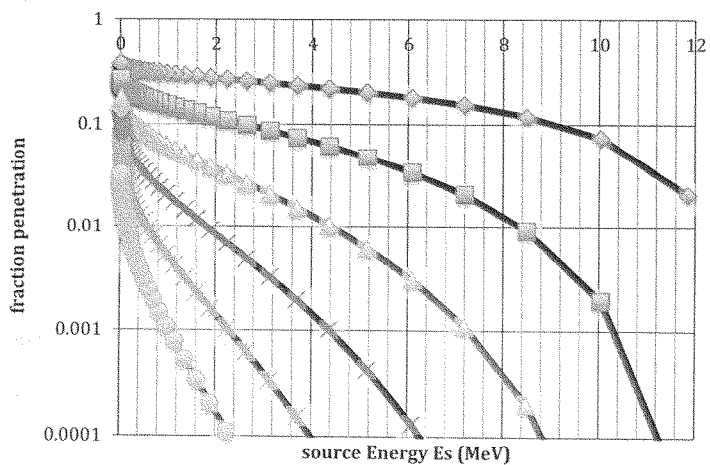


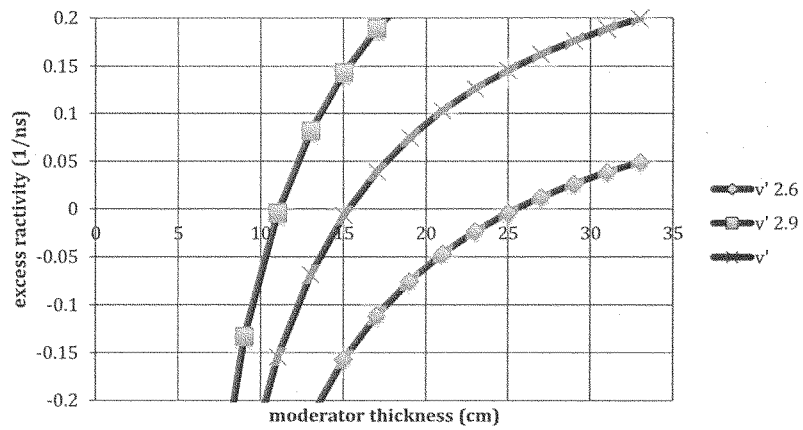
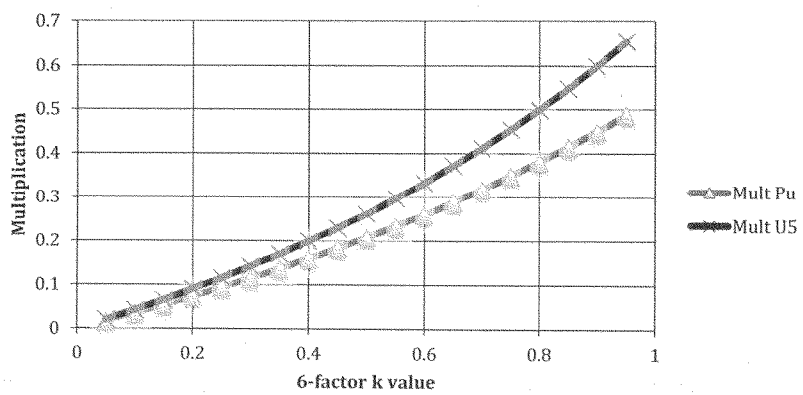
uranium. The probability of a fission is  $p$ ; the probability of 2 fissions in sequence is  $(pq)^2$ ; of 3 fissions in sequence is  $(pq)^3$ ; which sums to  $pq / (1-pq) < (f/v) / (1 - f/v)$  fissions, which for plutonium is  $\approx 0.5$  and for uranium  $\approx 0.7$ . Both are well below unity, so neutron interrogation could not produce criticality.

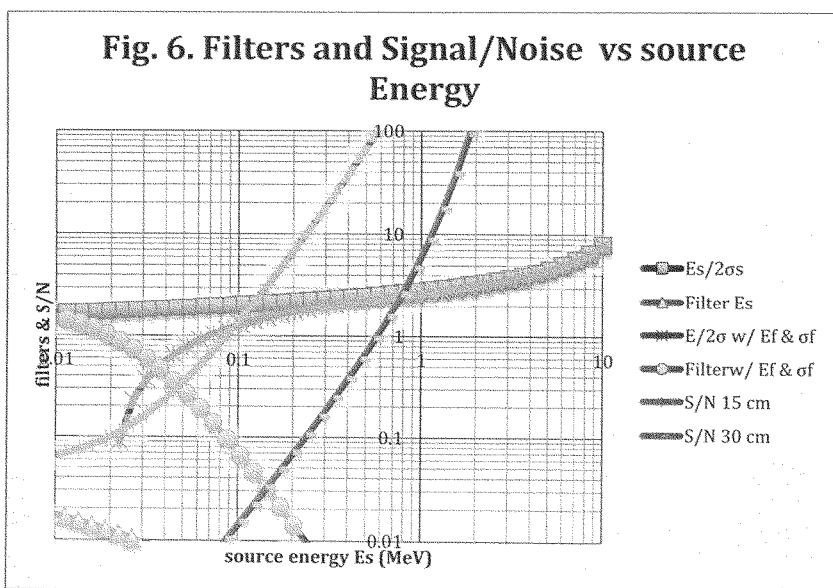
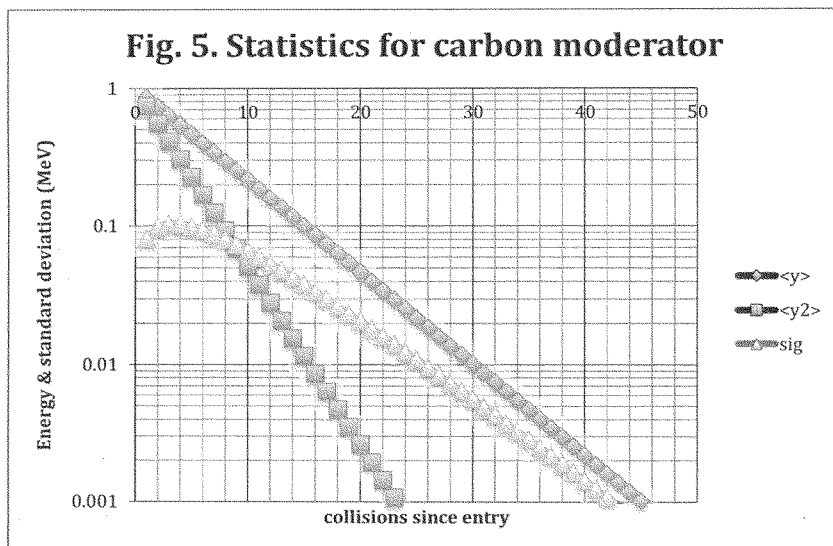
5. The energy  $E_F$  and standard deviation  $\sigma_F$  of fission neutrons fall exponentially with the total number of collisions experienced as they diffuse out through the moderator, by which both  $E_F$  and  $\sigma_F$  fall to  $\approx 1$  keV. Averaged over the slower fission rate collisions, the average  $E_F$  and  $\sigma_F$  are  $\approx 20$  and 6 keV.

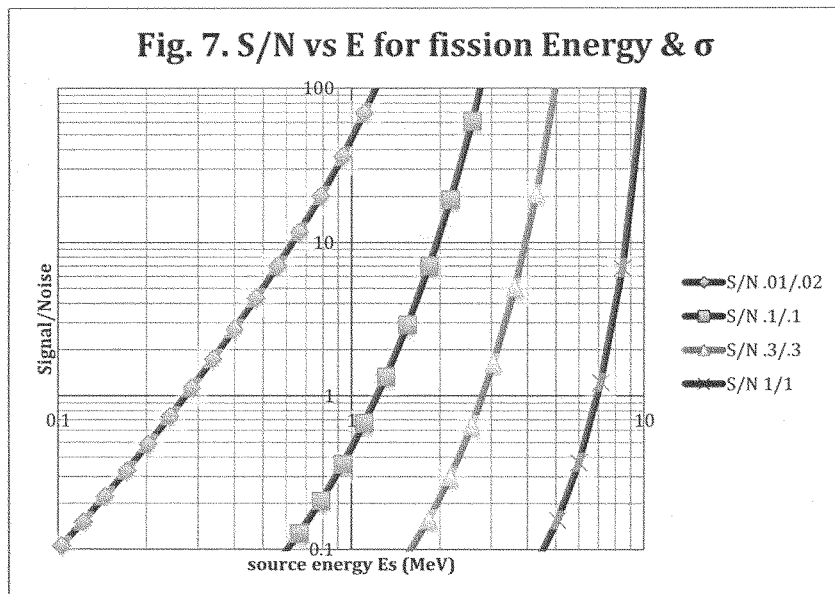
6. At energies  $>1$  MeV the source neutron energy  $E_S$  is much greater than  $E_F$ , and  $\sigma_F$  is small compared to standard deviation of source neutrons,  $\sigma_S$ , so the argument of the energy filter  $F$  reduces to  $E_S/2\sigma_S$ , which approaches 10 at the far right side of the figure the curve. There the argument including the fission statistics,  $(E_F - E_S)/2(\sigma_S + \sigma_F)$ , is similar. At energies below 0.1 MeV where the fission statistics become important, it falls rapidly, which defines the region of useful filter gain. The filter is  $F = 1 - \text{erf} [(E_F - E_S)/2(\sigma_S + \sigma_F)]$ ; the SNR is  $S/F$ , which is presented for signals  $S = 0.1$  for  $\approx 15$  cm moderators and 0.001 for 30 cm moderators, relative to unit sources. The SNR curve for 15 cm rises from  $\approx 0.1$  at 0.01 Me to  $\approx 100$  at 0.5 MeV, and that for 30 cm rises from  $\approx 0.01$  at 0.1 Me to  $\approx 100$  at 2 MeV, which are both large compared to those needed for high-confidence discrimination.

7. The signal to noise for the nominal parameters and a nominal signal of 0.1 is at left. The second curve results from increasing  $E_{SF}$  and  $\sigma_F$  arbitrarily by factors of 10; the second by 30; and the fourth by 100, which shift  $\text{SNR} = 100$  energies to 2, 4, and 10 MeV. While the source interactions take place at MeV energies, the discrimination measurements would be at keV energies at millisecond time scales.

**Fig. 1. Slowing down time vs Energy****Fig. 2. Penetration to Range vs Energy**

**Fig. 3. Criticality vs moderator thickness****Fig. 4. Multiplication for Pu & U vs 6-factor k**





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

On behalf of the  
American Association of Port Authorities (AAPA)

Before the Committee on Transportation and Infrastructure's Subcommittee on Coast Guard  
and Maritime Transportation and the Committee on Homeland Security's  
Subcommittee on Border and Maritime Security

Joint Hearing entitled  
An Examination of the Maritime Nuclear Smuggling Threat  
and Other Port Security and Smuggling Risks in the U.S.

Thursday, July 7, 2016  
10:00 a.m.  
2167 Rayburn House Office Building

Thank you Chairmen Hunter and McSally and Ranking Members Garamendi and Vela for convening this joint hearing. My name is David Espie, and I currently serve as the Director of Security for the Maryland Port Administration's Port of Baltimore. I am testifying today through the Committee's invitation and on behalf of the American Association of Port Authorities (AAPA) wherein I am a member of its Security Committee. This is a vital topic, which could ultimately impact the safety and security of the United States if not addressed in a cohesive and expedited manner.

The AAPA is the unified and collective voice of the seaport industry in the Americas. The AAPA empowers port authorities, maritime industry partners and service providers to serve their global customers and create economic and social value for their communities. AAPA activities, resources and partnerships connect, inform and unify seaport leaders and maritime professionals in all segments of the industry around the Western Hemisphere. Security is a top priority for all member seaports. This testimony is on behalf of our United States members.

In my role as the Director of Security for the Port of Baltimore, the prevention of maritime nuclear smuggling into the United States is a top priority that requires a multi-faceted approach. It requires the input of diplomatic resources, technical assets, human capital and appropriate funding to facilitate subsequent preventive methodologies. All of this requires a strong partnership with the federal government.

## AAPA Testimony on Nuclear Smuggling and Other Port Security Smuggling Risks

As a retired FBI agent and former National Security Agency (NSA) Special Agent, I also view our security from a national perspective that must empower ports to be more engaged in our national security apparatus.

In my experience, it is vital that our government have sound diplomatic relationships with countries that will cooperate with the United States in not only applying necessary security measures to secure their own nuclear materials, but also assist in countering a neighboring or regional country that may possess such material and have negative intentions against our nation or other nations. Global diplomacy and policies impacts local port security enforcement.

For example, the State Department's Counter Nuclear Smuggling Unit, Department of Energy's partnership has nearly 50 countries providing radiation detection and nuclear forensics equipment. The recent Nuclear Security Summit held here in Washington is an example of the technical assets of our intelligence and federal law enforcement agencies and must be staffed, continually deployed and refined. As we seem to see each day on the news, today's security threat is a fluid target that is neither stagnant nor bound to any particular country, region or territory, a church, an airport a night club, the list grows.

Existing capabilities and resources must be deployed and fully capable in order to maximize our country's opportunity to readily identify and neutralize potential threats. Development and tasking of domestic and international sources must remain a priority of our intelligence services and our local, state and federal law enforcement agencies. In some cases, I believe it would be beneficial for port security directors to receive FBI briefings.

As an example, the threat of maritime terrorist smuggling appears to be increasing, possibly in correlation with the flight of Syrian refugees to Europe. Recently, a stowaway on a roll-on roll-off vessel destined for Baltimore was located by the ship's crew and taken into custody by Homeland Security Investigations (ICE). The stowaway admitted that he boarded the vessel while it was docked at a German port.

Approximately one week prior to this event, a shipping lines manager in Baltimore advised that his lines had experienced several stowaway attempts by Syrian nationals in Germany as well. Directors of port security in the United States are not routinely granted a security clearance with the federal government and hence, are not provided classified briefings regarding threats to their ports.

The suspects of maritime nuclear smuggling efforts are numerous. The actions and aggressiveness of the Islamic State of Iraq and the Levant (ISIL) are challenging all aspects of our port security procedures. The threat from ISIL emerges on several fronts. First, the size of ISIL's force is substantial. Second, ISIL is not a congruent entity. Its leadership remains in a fractured state and subsequently, sub-factions form that are very difficult to identify or trace. Third, ISIL's

use of the internet and related systems to recruit both actual soldiers and lone wolves has proven to be extremely successful.

As a former police officer and now as a port security director, resources that can be utilized at the local level are vitally important. FEMA's Port Security Grant Program, has been instrumental in coordinating port specific security needs with the national and global threats.

AAPA encourages Congress to continue to fund the Port Security Grant Program, but also insists that grant funding be directed to ports and not diluted out to other law enforcement entities with very low threats. Funding to local law enforcement needs to illustrate a stronger connection with the port complex to ensure the funds are being used for their intended purposes. There should be a letter of endorsement from the port authority if a regional authority is to receive a port security grant. Threats against or nations seaports are always emerging and port security grants are in continual demand.

Cybersecurity is a prime example of an emerging security threat since 9/11. Ports are working with their stakeholders in addressing this very complex issue.

For example, in a recent survey of U.S. AAPA Security Directors:

- 52% of our ports have done a cybersecurity assessment within the last three years
- 67% of our ports Area Maritime Security Committee have formed a cybersecurity working group

Our ports meet with the following groups on cybersecurity:

- 97% have met with the Coast Guard
- 20% have met with terminal operators
- 6% with shippers
- 68% of ports of received port security grant funding to do a cyber assessment
- 63% have received PSG funding for ongoing cyber projects
- 100 port employees are dedicated to cyber (there are also some part-time employees dedicated to cyber)

In addition to cybersecurity, cargo containers have been identified as the most plausible mechanism for smuggling nuclear material into the United States. Over 11 million containers are shipped to our nation's 300 sea and river ports on an annual basis. With the recent completion of the Panama Canal expansion the number of containers from foreign ports will dramatically rise.



## AAPA Testimony on Nuclear Smuggling and Other Port Security Smuggling Risks

Following the 9/11 Commission, as you are aware, in 2007 Congress passed a law mandating that before a cargo container was shipped to the United States it must be scanned with imaging equipment and a radiation device.

To date, this law has not been procedurally incorporated wherein exemptions have been employed by the Department of Homeland Security (DHS). Recently, an additional two-year extension of the law's implementation was approved by DHS with the support of AAPA, 100 supply chain and industry stakeholders. It has been estimated that it would cost approximately \$20 billion to deploy scanning procedures and technology at the 700 foreign ports which ship cargo to the United States.

AAPA continues to work with DHS, stakeholders and industry experts in identifying innovative approaches in ensuring container security.

As many of you already understand, the primary responsibility to detect and/or deter maritime nuclear smuggling into the United States is Customs and Border Protection (CBP) and increasingly ports need the CBP boots on the ground.

CBP also incorporates two proactive programs in an effort to counter maritime nuclear smuggling, Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI). C-TPAT is an outreach program to elicit the cooperation of the maritime industry which now has over 10,000 certified partners. The CSI has three main focuses: identify high-risk containers, prescreen and evaluate containers prior to shipment and utilize technology to prescreen high-risk containers.

However, all containers leaving a port are screened by a Radiation Portable Monitor (RPM) wherein if an alert surfaces the container is subject to secondary screening. The 2006 Security and Accountability for Every Port Act mandated that the 22 largest container ports utilize RPMs.

The totality of CBP's RPM program is somewhat in a state of flux. First, the current RPM technology is dated. Second, the maintenance of RPMs in place appears to fluctuate-such maintenance records are not shared with port security directors. Third, although nothing has been officially related to ports, CBP has inferred that the costs of newly installed RPMs will be the burden of the port operator.

The current RPM program requires a thorough assessment and that CBP funding surrounding the performance and future implementation of this technology should ultimately be increased to cover necessary costs to include manpower as well.

In fiscal year 2015, when CBP was funded to hire 2,000 staff, fewer than 20 officers were assigned to seaports. We cannot let this disproportionate approach to security continue. Our

*AAPA Testimony on Nuclear Smuggling and Other Port Security Smuggling Risks*

nation's seaports handle more than 11 million maritime containers and over 11 million international passengers each year.

Representatives Forbes, Poe, Hahn and Castor recently led a letter signed by 47 members, requesting that more focus be placed on hiring maritime CBP staff. AAPA is submitting a copy of this letter for the record.

In summary, our nation's strategy to prevent maritime nuclear smuggling must utilize a holistic approach. This strategy should continue to incorporate diplomatic engagement; utilize intelligence community human and technical assets; a continued examination of port security protocols to include those of which are federally mandated and those imposed by port operators; increased funding of the Federal Emergency Management Agency's Port Security Grant Program to ensure ports are or remain in federal compliance; and the investment of appropriate funding levels for federal agencies, particularly CBP, in order for current and future legislative mandates be properly executed.

Thank you for the opportunity to testify this morning, and I look forward to any questions you may have.

**STATEMENT OF JAMES WEAKLEY, PRESIDENT,  
LAKE CARRIERS' ASSOCIATION, BEFORE A JOINT HEARING OF  
THE HOUSE TRANSPORTATION AND INFRASTRUCTURE COMMITTEE'S COAST  
GUARD AND MARITIME TRANSPORTATION SUBCOMMITTEE AND  
THE HOUSE HOMELAND SECURITY COMMITTEE'S MARITIME AND BORDER  
PROTECTION SUBCOMMITTEE  
10 a.m., July 7, 2016**

**“An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security  
and Smuggling Risks in the U.S.”**

Good morning. Thank you for the opportunity to speak to you today. I am Jim Weakley, president of the Lake Carriers' Association (LCA). We represent 14 American companies that operate 56 U.S.-flag vessels on the Great Lakes and carry the raw materials that drive the nation's economy: iron ore and flux stone for the steel industry, aggregate and cement for the construction industry, coal for power generation, as well as salt, sand and grain. Collectively, our members can transport more than 100 million tons of dry-bulk cargo per year and employ more than 1,600 men and women, all of whom are U.S. citizens or legally admitted aliens, and provide annual wages and benefits of approximately \$125 million. In turn, the cargos our members carry generate and sustain more than 103,000 jobs in the eight Great Lakes states and have an annual economic impact of more than \$20 billion.

I would like to provide a brief overview of the Great Lakes Navigation System (GLNS), its different market segments, risk profiles and mitigation strategies. Then I'll focus the majority of my testimony on how Lake Carriers' Association members work to transition their vessels from homeland security risks to homeland security resources. My comments will perhaps be broader than some of the other testifiers today, representing the views of private sector vessel owners.

***The GLNS***

The GLNS enables maritime commerce on America's Fourth Sea Coast. The five Great Lakes are tied together by three connecting channels (the St. Marys River, the Detroit/St. Clair River system and Welland Canal) and the so-called “Achilles heel of North American Manufacturing,” the locks at Sault Ste. Marie, Michigan. The St. Lawrence Seaway is the umbilical cord that connects the GLNS and its 68 U.S. ports and 35 Canadian ports to global trade. The Great Lakes are a bi-national system supporting both domestic and international trade. For example, the navigation channel crosses the U.S./Canadian border 17 times in the

Detroit/St. Clair River portion of the system alone. If measured as a single region, the eight Great Lakes States and two Canadian Provinces represent the world's third largest economy.

Although there is a great desire to move international container traffic to the GLNS, the majority of the cargo moved today is bulk. The ocean-going international fleet, vessels sometimes referred to as "salties," primarily bring steel into the Great Lakes region and take grain out. Approximately 225 salties call annually on both sides of the border moving 10 million tons of cargo a year.

"Lakers," the vessels LCA represents, are ships and barges specifically designed for the Great Lakes trade. Most are self-unloading dry-cargo vessels, although some lack the self-unloading equipment and others move liquid bulk material. Both the United States and Canada reserve their domestic waterborne movements of cargo for "coastwise qualified" vessels. Our nation's "Jones Act-qualified" vessels are American-owned, American-built and American-crewed. In 2013, U.S.-flag lakers transported about 86 million tons of iron ore, coal, limestone, cement, salt, sand and grain in purely domestic moves (between two U.S. points) under the Jones Act. Canadian-flag lakers transported slightly more than 35 million tons of cargo domestically (between two points in Canada), including Canadian points on the Great Lakes ports, the Canadian Arctic or its East Coast.

The Canadian and American fleets compete for the Great Lakes' binational cross-lake cargo. In 2013, the last year for which complete data is available, the total cross-lake trade represented 37.4 million tons of cargo. The Canadian-flag fleet carried 34.6 million of it, representing about 93% of the total. The U.S.-flag fleet carried 2.8 million tons or about 7%.

#### ***Great Lakes Security Risk Profile***

LCA members are the linchpin of what has been called "[o]ne of the nation's most economically vital systems, the iron mining—integrated steel production—manufacturing supply chain..."<sup>1</sup> In general, iron ore, the primary raw material for steel, is transported by our ships from mines in Minnesota and the Upper Peninsula of Michigan to steel mills in Indiana, Ohio, Michigan and Pennsylvania. So crucial is that waterborne supply chain that the Department of Homeland Security (DHS) has warned that an interruption of domestic shipping services through the Poe Lock at Sault Ste. Marie, Michigan, would have "catastrophic impacts on the regional and National economy,"<sup>2</sup> including the interruption of steel production and the plunging of the North American economy into a "severe recession."<sup>3</sup>

The DHS study estimated that 11 million Americans would become unemployed and 3–5 million Mexicans and Canadians would lose their jobs if shipping through the Poe Lock was interrupted for a six-month period beginning at the start of the shipping season. This is both a

<sup>1</sup> "The Perils of Efficiency: An Analysis of an Unexpected Closure of the Poe Lock and its Impact," Department of Homeland Security, (October, 2015), at 1. While this report is focused on the impact of a failure of the Soo Lock, through which vessel that are part of this supply chain must pass, the analysis also demonstrates the significant impact of shipping on the Great Lakes economy and beyond.

<sup>2</sup> *Id.* at 29.

<sup>3</sup> *Id.* at iii.

direct and indirect result of the manufacturing made possible by the 60 million tons of key raw materials transiting the Poe Lock, part of the Soo Lock system, on an annual basis. According to DHS, the State of Michigan's unemployment would reach 22%, so exceeding its peak unemployment rate of 15% during the Great Recession.

However, this is a national problem. In fact, the unemployment spikes in the event of an interruption in Great Lakes shipping will ripple through the United States, a result of the far-reaching impacts of the automobile manufacturing and general steel industry. The Army Corps of Engineers (the "Corps"), which operates the Poe Lock, has taken security measures to ensure the protection of the Lock. However, LCA and many others believe that the risk requires construction of a lock that is redundant to the Poe. To its credit, the Corps is undertaking an "Economic Reevaluation Report" (ERR) to update the redundant lock's benefit-to-cost ratio (BCR). The ERR will correct some flawed assumptions in the previous BCR; however, it will not consider the impact of millions of unemployed North Americans. It will only consider the "first order of magnitude impacts" such as the cost to vessels that would have carried the ore. The ERR should be completed by December of 2017, which means the earliest the Corps is likely to begin construction on this ten-year project is FY 20. Like DHS, we believe the strategic importance of the project deserves more attention.

All of that is simply to say that the threat of port and other maritime security risks on the Great Lakes are matters of great concern not just for our industry but also for our nation.

#### ***This Hearing***

While the House Transportation and Infrastructure Committee and its Coast Guard and Maritime Transportation Subcommittee have always had primary jurisdiction over our issues, there is a tremendous growing national interest in the intersection between our maritime industry and homeland security. As you well know, the length of our nation's water borders far exceeds its land borders, which receive so much more public attention. Therefore, the jurisdiction of the Homeland Security Committee and its Maritime and Border Protection Subcommittee has taken on a role of increased importance as our nation battles smuggling and related issues of all kind. In fact, here's what the Coast Guard has said about the potential vulnerability through our water borders:

The vastness of this system and its widespread and diverse critical infrastructure leave the nation vulnerable to terrorist acts within our ports, waterways, and coastal zones, as well as exploitation of maritime commerce as a means of transporting terrorists and their weapons.<sup>4</sup>

The Great Lakes provide an interesting study on the importance of maritime homeland security. Although much of the national attention is focused on the southern border of the United States, the northern border faces challenging issues of its own. The southern land border of the United States is about 2,000 miles long. However, the Canadian/U.S. border is about

---

<sup>4</sup>Testimony of Rear Admiral Joseph Servidio, Assistant Commandant for Prevention Policy, before the House Coast Guard and Maritime Transportation Subcommittee, at a hearing titled, "Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer?", September 11, 2012.

5,500 miles long, almost three times as long, and much of that U.S./Canadian border is a water border.

As you can imagine, there are many maritime security issues related to that extensive water border, and we deal with a complex series of interlocking rules and requirements in a world where ships from Canada and around the world move seamlessly between U.S. and Canadian waters. All those laws and regulations play an important role in border security, but, from a practical point of view, one law stands above all others for its impact on American maritime homeland security—the federal law known as the Jones Act.

### *The Jones Act*

The Jones Act, of course, is the fundamental law of the American maritime industry. It requires that any cargo moving between two points in the United States be carried on U.S.-built, U.S.-crewed and U.S.-owned vessels. In other words, American vessels!

Most people on these Subcommittees know that the Jones Act provides important national security and economic benefits. But there is overwhelming evidence that one of the most important benefits of the Jones Act is homeland security, which includes prevention of illegal smuggling but also much more. While the Jones Act is not primarily a homeland security law, its role in keeping our nation secure is significant. Former U.S. Senator Slade Gorton, a former Washington State attorney general and member of the 911 Commission, recently wrote that “helping to plug a porous border is a benefit of the Jones Act that is far too often overlooked.” *Strengthening Border Security: Look No Further Than the Jones Act*, The Hill, February 12, 2016. Likewise, Dr. Daniel Goure of the Lexington Institute, a prominent think tank, has prepared two studies recently, including one titled, *Venerable Jones Act Provides an Important Barrier to Terrorist Infiltration of the Homeland*, Lexington Institute, March 24, 2016. He said, “Since 911, the Jones Act has taken on new significance in a way no one ... could have imagined. It now plays an important role in securing the homeland from the threat of international terrorism.” *The Jones Act and Homeland Security in the 21st Century*, Lexington Institute, June 2016.

Dr. Goure points out that the land borders in America are “dwarfed by 95,000 miles of the national shoreline.” He points out that there are 25,000 miles of navigable waterways in our nation’s inland river system. Of course, many cities in America, large and small, are located along this shoreline. That is certainly true on the Great Lakes.

Of course, virtually all of the vessels that operate in the inland waterways and many of the vessels on the Great Lakes are Jones Act vessels. There are approximately 40,000 Jones Act vessels across the United States. On the Lakes, our fleet includes very large vessels, including ships as large as an aircraft carrier. The homeland security benefit of these Jones Act vessels is noteworthy.

Let me quote directly from one of Dr. Goure’s studies:

The task of securing U.S. seaports and foreign cargoes is daunting by itself. It makes no sense to add to the burden facing domestic security agencies by allowing foreign-owned ships operated by foreign crews to move freely throughout America's inland lakes, rivers and waterways. The requirement that all the officers and fully 75 percent of the crews of vessels engaged in cabotage be U.S. citizens goes a long way to reducing the risk that terrorists could get onboard or execute an attack on a U.S. target. In effect, there is a system of self-policing that reduces the requirement for law enforcement and homeland security organizations to expend time and effort to ensure that these vessels and crews are safe to traverse U.S. waters. Were the Jones Act not in existence, the Department of Homeland Security would be confronted by the difficult and very costly requirement of monitoring, regulating and overseeing foreign-controlled, foreign-crewed vessels in coastal and internal U.S. waters.<sup>5</sup>

My comments, of course, should not be read as an indictment of all foreign shipping companies that come in and out of the United States, including in and out of the Great Lakes. Obviously the overwhelming majority of those companies, vessels and seafarers are not a security threat to the United States. My point is simply that vessels owned and crewed by Americans under the Jones Act have a very different risk profile than foreign vessels. For example, our Jones Act mariners have all gone through extensive background checks in order to receive their licenses, credentials and Transportation Worker Identification Credential (TWIC) cards. Many have been trained at our maritime schools and universities. They live here. They work here. These mariners and the companies they work for are fully subject to the reach of our legal and regulatory system. In fact, many of these mariners and companies are full partners with our American law enforcement agencies through a series of programs and partnerships that encourage American seafarers to report suspicious activities, as discussed further below.

The opposite situation occurs when a foreign vessel with a foreign crew enters a U.S. port. Because those crew members do not live and work here and sometimes are completely unknown to us, there is a system of regulations and requirements to identify and address potential threats. That regulatory system is elaborate, very expensive and, by definition, imperfect. Unfortunately, in some cases we must rely on the screening practices of foreign nations. That's why, according to the U.S. Government Accountability Office, "The Department of Homeland Security (DHS) considers the illegal entry of an alien through a U.S. seaport by exploitation of maritime industry practices to be a key concern."<sup>6</sup>

So if you ask me what the single most important thing you can do to encourage maritime homeland security, I would say support the Jones Act. I have worked as an officer in the Coast Guard, for an American shipping company and now heading an association of American shipping companies, and from every vantage point I have seen that the Jones Act is our best line of maritime homeland security defense.

<sup>5</sup> "Venerable Jones Act Provides an Important Barrier to Terrorist Infiltration of the Homeland (Goure).

<sup>6</sup> "GAO-11-195, Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened", [www.gao.gov](http://www.gao.gov). Retrieved 2016-06-24

*Other Great Lakes Security Issues and Practices*

The Jones Act is just one of many protections to prevent smuggling and other nefarious activity in the maritime sector. From the perspective of a U.S.-flag Great Lakes vessel operator, our goal is to reduce our vulnerability to all threats as much as possible. As mentioned earlier, our primary homeland security objective is to go from being a homeland security risk to homeland security resource. Here are a few of the many ways that we do that:

National and Regional Risk Profile — Risk is a combination of threat and vulnerability. Others on this panel and the previous one are far more qualified to comment on threat than I am. In fact, our companies depend on the Coast Guard to notify us regarding the current and changing homeland security threat status by its system of “Maritime Security Threat Levels” or “MARSEC.” If the Coast Guard decides to change the threat level based on information in its possession, it notifies us, company security officers and vessel security officers. Once that notification is made, the appropriate action is taken as prescribed in company and vessel security plans. Our relationship with the Coast Guard is highly cooperative.

The second aspect of risk is vulnerability. From vessel perspective, there are both internal and external vulnerabilities. Both of these types are specifically addressed based on the aforementioned individual vessel security assessment and response plans. LCA’s members use the Coast Guard approved “Alternative Security Program for Great Lakes Dry-Bulk Cargo Vessels.” Since the plan is considered “Sensitive Security Information” in accordance with Title 49 of the U.S. Code of Federal Regulations, I will not go into great detail. From a general perspective, we deploy many of the security measures you would expect, including access control, perimeter expansion, personnel screening, vessel security sweeps, random baggage searches and inspection of cargo and ship stores. We not only adjust our security profile based on the prescribed threat level but also on the vessel operations and operational area. For example, if the vessel is moored at a facility that is not required to comply with facility security regulations, undergoing winter maintenance, in long-term storage or operating in restricted waters, we may also adjust our security profile. These types of programs and systems are a core part of how we operate.

Great Lakes Military and Law Enforcement — Obviously, vessel owners, operators and crew form only a piece of the national maritime strategy to prevent smuggling and other threats. The task given our military and law enforcement agencies, including the Coast Guard and Customs and Border Protection in the United States, can be daunting. Using credible intelligence these officials deploy their resources to conduct safety inspections, scrub crew lists, review manifests and conduct full scale law enforcement boardings. The use of random inspections is another tool, and our crews are often subjected to a level of scrutiny that they had not experienced prior to the global war on terror. Our sailors understand the greater national security interests at stake and cooperate with and have the highest regard for American law enforcement agencies like the Coast Guard. We also work with law enforcement agencies to make our vessels available as training platforms both while underway and during maintenance periods.

“Eyes on the Water” — In the wake of the terrorist attacks at the World Trade Center in New York, the Coast Guard has formalized a program that encourages professional mariners to report



suspicious activity on the water. Through its “Eyes on the Water” program, the Coast Guard recognized that the more eyes looking, the better, and who could be more qualified to recognize that something is afoul than the professionals who routinely sail the trade routes. All of our members participate and report unusual or suspicious activity (e.g., when an unmanned aerial vehicle buzzes a vessel or a critical piece of infrastructure). These are low cost, common sense programs that make our homeland more secure, and we are proud to be full partners.

Radar Remote Access — Several LCA members are cooperating with a vendor on a project that we think could benefit both law enforcement and search and rescue responders. The program records vessel radar pictures with automatic identification system (AIS) data and allows shore based operators to remotely access the information. We believe the system, if proven successful, could be used to identify patterns of suspicious activity. Radars can monitor “uncooperative” aircraft and vessels that are not required to or choose not to transmit AIS data. Having the ability to look at a series of historical radar screens in an area can reveal suspicious trends and having real time access to remotely look at a radar picture from a vessel underway vastly expands the ability of shore based monitoring systems.

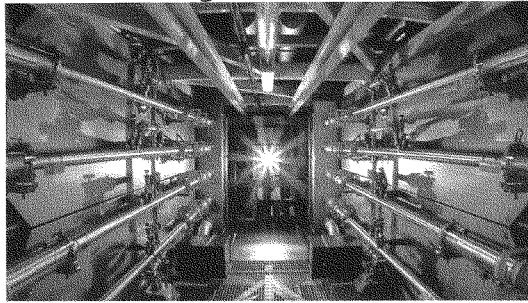
Mitigation for Salties — Great Lakes pilotage regulations require salties to carry a Canadian or American registered pilot while sailing in the Great Lakes. Other U.S. states have similar pilotage requirements for vessels entering America on international voyages. Although the primary job of the pilot is to provide the vessel master with navigation advice, pilots also perform a vital security function. Often they are the only American aboard a foreign vessel and well-positioned to alert the Coast Guard or other law enforcement officials of suspicious activity or unusual cargo aboard a foreign vessel in our waters destined for our docks. Highly trained American pilots provide an onboard set of eyes with a vested interest in protecting our homeland.

### ***Conclusion***

In today’s world, threats to our maritime security are daunting. Every day our LCA companies, and many other companies like them, are executing security plans, cooperating with law enforcement, implementing innovative new programs, operating under the highly beneficial requirements of the Jones Act and, ultimately, working to transition from a security risk to a security resource. This is our goal every single day both as American shipping companies and as America citizens.

Thank you for your interest and for the opportunity to provide my perspective. I am happy to answer any questions you may have.

## U.S. Ports Want More Action on Dirty Bomb Prevention



By **MarEx** 2016-07-06 18:59:32

The threat of terrorist smuggling at U.S. ports appears to be increasing, says the American Association of Port Authorities (AAPA), who wants mechanisms to prevent cyber terrorism and illegal nuclear materials from being trafficked through ports intensified.

Nuclear smuggling can involve small quantities of highly enriched uranium or plutonium that could be used to build an improvised nuclear device. Additionally, radiological materials, such as cesium-137, cobalt-60, and strontium-90, can be combined with conventional explosives to build a radiological dispersal device, often referred to as a dirty bomb.

According to a nuclear and radiological material trafficking database managed by the International Atomic Energy Agency (IAEA), approximately 2,700 cases of illicit trafficking of such material have been confirmed as of December 31, 2014. These cases were reported by more than 100 countries that voluntarily contribute to IAEA's database.

Many confirmed cases involving the illicit trafficking of nuclear materials, including weapons-usable material, have been traced to material that originated in countries of the former Soviet Union and had fallen outside of those governments' control.

Maryland Port Administration Security Director Dave Espie, a retired FBI agent and former National Security Agency Special Agent, will testify on July 7 on behalf of the AAPA at a joint hearing of the House Transportation and Infrastructure Committee's Subcommittee on Coast Guard and Maritime Transportation, and the House Homeland Security Committee's Subcommittee on Border and Maritime Security.

Espie says in his testimony that the threat of maritime terrorist smuggling appears to be increasing, possibly in correlation with the flight of Syrian refugees to Europe. Recently, a

stowaway on a roll-on rolloff vessel destined for Baltimore was located by the ship's crew and taken into custody by Homeland Security Investigations. The stowaway admitted that he boarded the vessel while it was docked at a German port.

Approximately one week prior to this event, a shipping lines manager in Baltimore advised that his lines had experienced several stowaway attempts by Syrian nationals in Germany as well. Directors of port security in the United States are not routinely granted a security clearance with the federal government and hence, are not provided classified briefings regarding threats to their ports, says Espie.

The suspects of maritime nuclear smuggling efforts are numerous, says Espie. "The actions and aggressiveness of the Islamic State of Iraq and the Levant (ISIL) are challenging all aspects of our port security procedures. The threat from ISIL emerges on several fronts. First, the size of ISIL's force is substantial. Second, ISIL is not a congruent entity. Its leadership remains in a fractured state and subsequently, sub-factions form that are very difficult to identify or trace. Third, ISIL's use of the internet and related systems to recruit both actual soldiers and lone wolves has proven to be extremely successful."

Maritime nuclear smuggling "could ultimately impact the safety and security of the United States if not addressed in a cohesive and expedited manner," says Espie in his testimony.

Espie believes there is a need for sound diplomatic relationships with nations that cooperate with the U.S. to secure their own nuclear materials, and the need for them to assist in countering ambitions of nuclear countries intent on inflicting harm with their fissionable materials.

In his prepared statement, Espie says that the U.S. strategy to prevent maritime nuclear smuggling should use a holistic approach that incorporates diplomatic engagement, utilizes intelligence community assets (human, cyber and technical), focuses on port security protocols (both federally mandated and those imposed by port operators), increases Port Security Grant funding to ensure ports are brought up to and remain in federal compliance, and appropriately invest in federal agencies like Customs and Border Patrol to ensure current and future legislative mandates are properly executed.

His testimony encourages Members of Congress to continue funding ports and that Customs and Border Patrol assign more than one percent of its new hires to seaports, which was the approximate staffing ratio of Customs and Border Patrol new hires to ports in fiscal year 2015.

In June, the United States Government Accountability Office submitted a report to the Subcommittee on Energy and Water Development, Committee on Appropriations, U.S. Senate on U.S. actions combatting nuclear smuggling. The report confirms that international nuclear and radiological smuggling threatens the security of the United States.

The report highlights the global nature of the issues, and states that, according to officials from the Department of Homeland Security, detecting and interdicting such materials as close to the original source - and as far away from the United States - as possible, increases the probability of successfully deterring nuclear smuggling into the United States and strengthens national security.

**Congress of the United States**  
**House of Representatives**  
**Washington, DC 20515**

July 1, 2016

The Honorable Jeh Johnson  
 Secretary of the Department of Homeland Security  
 U.S. Department of Homeland Security  
 Washington, D.C. 20528

Dear Secretary Johnson:

Thank you for your service and your dedication to protecting and securing our country. We recognize and support your Department's ongoing efforts to improve security and alleviate passenger wait-times in our nation's airports. However, as you are well aware, our nation's security is a multi-faceted challenge. As DHS addresses the ongoing challenges associated with aviation security, we ask that you also focus long overdue resources to our maritime ports and resolve the Customs and Border Protection (CBP) staffing shortages facing the passenger and freight facilities that connect directly with our communities.

In Fiscal Year 2015, when CBP was funded to hire 2,000 staff, fewer than 20 officers were assigned to seaports. We cannot let this disproportionate approach to security continue. Our nation's seaports handle more than 11 million maritime containers and over 11 million international passengers each year. Annual increases in volume and periodic surges in ship traffic, paired with a muted response from the Department, have led to repeated dock-side delays in inspecting and clearing cargo, creating a ripple effect throughout our economy and supply chain.

To address these shortages, port authorities have utilized an array of tools to keep cargo and passengers moving through their terminals. One such tool is the congressionally authorized pilot 559 program, which allows ports to pay the overtime costs of CBP personnel when additional hours of screening are required. While this flexibility was meant to serve as an avenue for relief, it is not a cost that our ports can afford to bear in the long-term. The need for a permanent solution remains.

Moreover, as Members of Congress we stand ready and willing to assist the Department in addressing CBP's current staffing issues. In April, the House unanimously approved legislation to help enhance the operational capacity of CBP services with the passage of the Border and Maritime Coordination Improvement Act, H.R. 3586. Language was also included in the Fiscal Year 2017 National Defense Authorization Act (NDAA) to enable CBP to expedite the hiring process for applicants with a military background. These are important steps in the right direction; however, more must be done to ensure that the staffing shortages at our seaports are addressed.

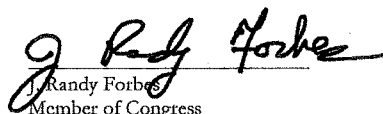
We, therefore, urge you to take this opportunity to address CBP staffing issues at our nation's seaports, in addition to our air and land ports of entry.

Thank you for your attention to this matter, and we look forward to your response.

Sincerely,



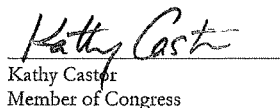
Ted Poe  
Member of Congress



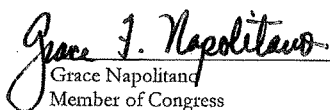
Randy Forbes  
Member of Congress



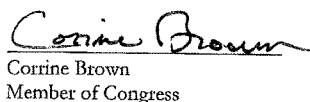
Janice Hahn  
Member of Congress



Kathy Castor  
Member of Congress



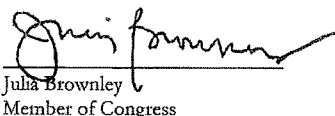
Grace Napolitano  
Member of Congress



Corrine Brown  
Member of Congress



Gene Green  
Member of Congress



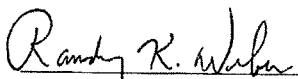
Julia Brownley  
Member of Congress



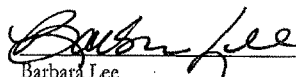
Alan Lowenthal  
Member of Congress




Scott Peters  
Member of Congress



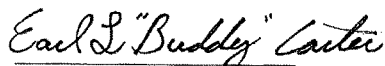
Randy Weber  
Member of Congress



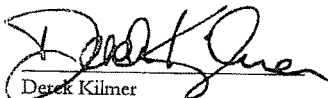
Barbara Lee  
Member of Congress



Brenda L. Lawrence  
Member of Congress



Earl L. "Buddy" Carter  
Member of Congress



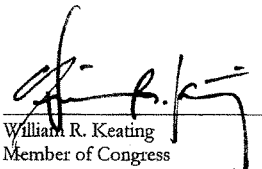
Derek Kilmer  
Member of Congress



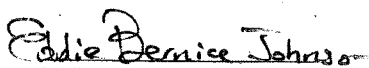
Stacey E. Plaskett  
Member of Congress



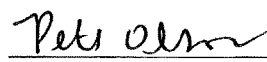
Brian Babin  
Member of Congress



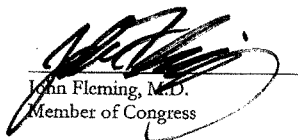
William R. Keating  
Member of Congress



Eddie Bernice Johnson  
Member of Congress



Pete Olson  
Member of Congress



John Fleming, M.D.  
Member of Congress



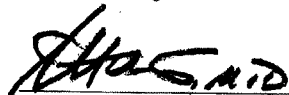
Scott Rigell  
Member of Congress



Blake Farenthold  
Member of Congress



Bradley Byrne  
Member of Congress



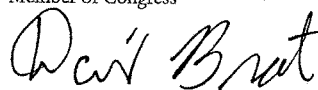
Andy Harris  
Member of Congress



Rob Wittman  
Member of Congress



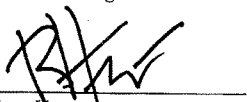
Bobby Scott  
Member of Congress



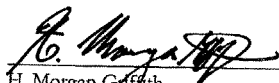
David Brat  
Member of Congress



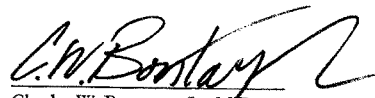
Barbara Comstock  
Member of Congress




Robert Hurt  
Member of Congress




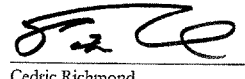
H. Morgan Gaffith  
Member of Congress

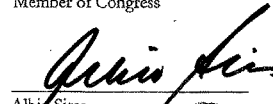



Charles W. Boustany, Jr., M.D.  
Member of Congress

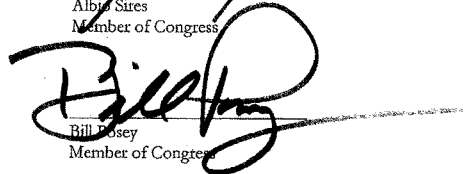
  
John Garamendi  
Member of Congress

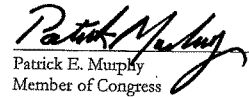
  
Robert Goodlatte  
Member of Congress

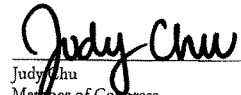
  
Cedric Richmond  
Member of Congress


  
Albio Sires  
Member of Congress

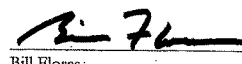
  
Al Green  
Member of Congress

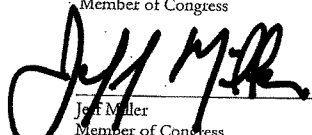
  
Bill Posey  
Member of Congress

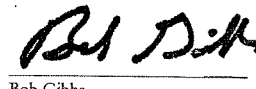
  
Patrick E. Murphy  
Member of Congress

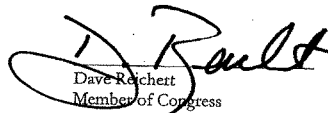
  
Judy Chu  
Member of Congress

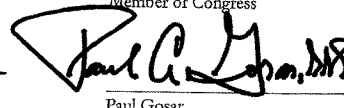
  
Frank C. Guinta  
Member of Congress

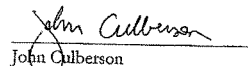
  
Bill Flores  
Member of Congress

  
Jeff Miller  
Member of Congress

  
Bob Gibbs  
Member of Congress

  
Dave Reichert  
Member of Congress

  
Paul Gosar  
Member of Congress

  
John Culberson  
Member of Congress

CC:

The Honorable John Carter, Chairman Homeland Security Appropriations Subcommittee

The Honorable Lucille Roybal-Allard, Ranking Member Homeland Security Appropriations Subcommittee

The Honorable John Hoeven Chairman Senate Committee on Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen, Ranking Member, Senate Committee on Appropriation Subcommittee on Homeland Security